

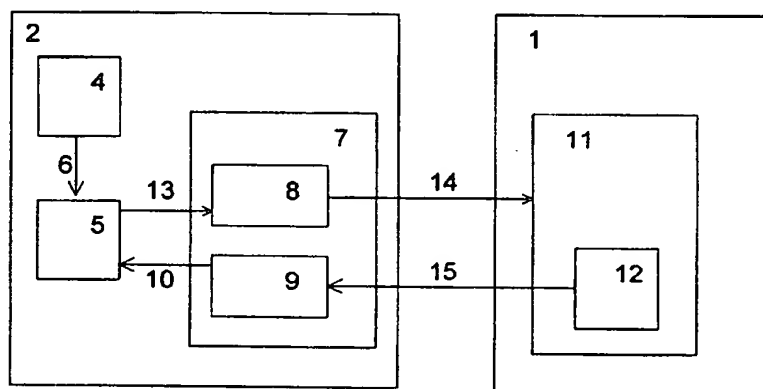


МЕЖДУНАРОДНАЯ ЗАЯВКА, ОПУБЛИКОВАННАЯ В СООТВЕТСТВИИ С
ДОГОВОРом О ПАТЕНТНОЙ КООПЕРАЦИИ (РСТ)

<p>(51) Международная классификация изобретения⁷: G07F 7/10</p>	<p>A1</p>	<p>(11) Номер международной публикации: WO 00/31700 (43) Дата международной публикации: 2 июня 2000 (02.06.00)</p>
<p>(21) Номер международной заявки: PCT/RU99/00264 (22) Дата международной подачи: 29 июля 1999 (29.07.99) (30) Данные о приоритете: 98120922 25 ноября 1998 (25.11.98) RU (71) (72) Заявители и изобретатели: ЗОЛОТОРЁВ Олег Анатольевич [RU/RU]; 188537 Ленинградская обл., Сосновый Бор, ул. Молодёжная, д. 25, кв. 20 (RU) [ZOLOTOREV, Oleg Anatolievich, Sosnovy Bor (RU)]. КУЗНЕЦОВ Иван Владимирович [RU/RU]; 191123 Санкт-Петербург, ул. Салтыкова-Щедрина, д. 48, кв. 56 (RU) [KUZNETSOV, Ivan Vladimirovich, St.Petersburg (RU)]. МОШОНКИН Андрей Геннадьевич [RU/RU]; 191123 Санкт-Петербург, ул. Шпалерная, д. 44а, кв. 5 (RU) [MOSHONKIN, Andrei Gennadievich, St.Petersburg (RU)]. СМIRHOV Александр Леонидович [RU/RU]; 191126 Санкт-Петербург, ул. Достоевского, д. 36, кв. 8 (RU) [SMIRNOV, Alexandr Leonidovich, St.Petersburg (RU)]. ХАМИТОВ Ильдар Магафурович [RU/RU]; 193029 Санкт-Петербург, ул. Бабушкина, д. 29, корп. 2, кв. 45 (RU) [KHAMITOV, Ildar Magafurovich, St.Petersburg (RU)].</p>		<p>(74) Агент: МАТВЕЕВА Татьяна Ивановна; 199034 Санкт-Петербург, Университетская наб., д. 7/9, Университет, Департамент патентов и лицензий (RU) [MATVEEVA, Tatiyana Ivanovna, St.Petersburg (RU)]. (81) Указанные государства: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, европейский патент (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), евразийский патент (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), патент ARIPO (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), патент OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG). Опубликована С отчётом о международном поиске. С изменённой формулой изобретения.</p>

(54) Title: METHOD FOR CARRYING OUT TRANSACTIONS AND DEVICE FOR REALISING THE SAME

(54) Название изобретения: СПОСОБ ПРОВЕДЕНИЯ ПЛАТЕЖЕЙ И УСТРОЙСТВО ДЛЯ ЕГО РЕАЛИЗАЦИИ



(57) Abstract

The present invention relates to a method for carrying out transactions and, during transactions on open telecommunication networks, for protecting the financial interests of each participant in the transaction against unauthorised actions by other participants. This method is used for protecting the privacy between payers and recipients and for carrying out transactions ranging from micro-transactions to business transactions, the transactions being subordinated in time to the rapidity of action of the network connections only regardless of the transaction amount. This method also allows to serve a number of clients that increases proportionally with the resources of the transaction system operator, can be easily integrated in any trade system, allows each client to make and receive payments and can be used for making transactions between the clients of different banks. This method for carrying out transactions is implemented in a software environment.

Предложен способ проведения платежей, который позволяет при проведении платежей по открытым телекоммуникационным сетям обеспечить защиту денежных интересов каждого участника платежа от злоупотреблений других участников, обеспечивает защиту приватности плательщиков и получателей, допускает платежи в диапазоне от микроплатежей до платежей бизнес-уровня, обеспечивает зависимость времени проведения платежа только от быстроты действия сетевых соединений, но не от величины платежа, допускает возможность обслуживания такого числа клиентов, которое растет пропорционально ресурсам оператора платежной системы, легко встраивается в произвольную торговую систему, обеспечивает возможность каждого клиента как платить, так и принимать платежи, допускает возможность проведения платежей между клиентами различных банков. Способ проведения платежей реализуется с помощью программных средств.

ИСКЛЮЧИТЕЛЬНО ДЛЯ ЦЕЛЕЙ ИНФОРМАЦИИ

Коды, используемые для обозначения стран-членов РСТ на титульных листах брошюр, в которых публикуются международные заявки в соответствии с РСТ.

AL	Албания	ES	Испания	LS	Лесото	SK	Словакия
AM	Армения	FI	Финляндия	LT	Литва	SN	Сенегал
AT	Австрия	FR	Франция	LU	Люксембург	SZ	Свазиленд
AU	Австралия	GA	Габон	LV	Латвия	TD	Чад
AZ	Азербайджан	GB	Великобритания	MC	Монако	TG	Того
BA	Босния и Герцеговина	GE	Грузия	MD	Республика Молдова	TJ	Таджикистан
BB	Барбадос	GH	Гана	MG	Мадагаскар	TM	Туркменистан
BE	Бельгия	GN	Гвинея	MK	бывшая югославская Республика Македония	TR	Турция
BF	Буркина-Фасо	GR	Греция	ML	Мали	TT	Тринидад и Тобаго
BG	Болгария	HU	Венгрия	MN	Монголия	UA	Украина
BJ	Бенин	IE	Ирландия	MR	Мавритания	UG	Уганда
BR	Бразилия	IL	Израиль	MW	Малави	US	Соединённые Штаты Америки
BY	Беларусь	IS	Исландия	MX	Мексика	UZ	Узбекистан
CA	Канада	IT	Италия	NE	Нигер	VN	Вьетнам
CF	Центрально-Африкан- ская Республика	JP	Япония	NL	Нидерланды	YU	Югославия
CG	Конго	KE	Кения	NO	Норвегия	ZW	Зимбабве
CH	Швейцария	KG	Киргизстан	NZ	Новая Зеландия		
CI	Кот-д'Ивуар	KP	Корейская Народно- Демократическая Рес- публика	PL	Польша		
CM	Камерун			PT	Португалия		
CN	Китай	KR	Республика Корея	RO	Румыния		
CU	Куба	KZ	Казахстан	RU	Российская Федерация		
CZ	Чешская Республика	LC	Сент-Люсия	SD	Судан		
DE	Германия	LI	Лихтенштейн	SE	Швеция		
DK	Дания	LK	Шри Ланка	SG	Сингапур		
EE	Эстония	LR	Либерия	SI	Словения		

СПОСОБ ПРОВЕДЕНИЯ ПЛАТЕЖЕЙ И УСТРОЙСТВО ДЛЯ ЕГО РЕАЛИЗАЦИИ

Область техники

Изобретение относится к области электронных платежных систем.

Предшествующий уровень техники

5 Электронные платежные системы предназначены для того, чтобы предоставить адекватное платежное средство для проведения сделок по открытым коммуникационным сетям. Помимо безопасности, надежности, стоимости обслуживания, быстродействия и т. п., важной характеристикой платежной системы является защита приватности пользователей.

10 Приватность пользователя предполагает, что никто, в том числе и оператор платежной системы, не в состоянии контролировать покупки пользователя. Один из способов защиты приватности в электронных платежных системах состоит в том, что покупки совершают с помощью цифровых данных, которые подтверждают платежеспособность, но не ведут к идентификации личности плательщика. Такие данные иногда называют электронными наличными. Однако электронные наличные, как и любые цифровые данные, легко копируются, что требует заботы о предотвращении их многократного использования.

В некоторых платежных системах многократное использование предотвращается платежным устройством плательщика (S. Brands, Untraceable Off-Line Cash in Wallets with Observers, Advances in Cryptology CRYPTO '93, Springer-Verlag, p. 302-318). Для надежного предотвращения многократного использования такие платежные устройства должны быть невзламываемы, то есть должны предотвращать непредусмотренный доступ к содержащимся в устройстве данным. Недостаток систем, использующих такой подход, состоит в их крайней неустойчивости. Дело в том, что взлом одного платежного устройства может привести к катастрофическим последствиям для всей системы, так как содержащиеся в платежном устройстве данные позволяют тратить произвольные необеспеченные суммы денег. Известные технологии конструирования невзламываемых устройств не столь надежны, чтобы оправдать такой риск.

Электронные платежные системы, не полагающиеся на невзламываемость платежных устройств, помимо прочего, должны обеспечить и неподделываемость платежных сертификатов, то есть цифровых данных, подтверждающих платежеспособность плательщика. Неподделываемость обеспечивается криптографическими методами, а именно, цифровой подписью оператора платежной системы. Многочисленные примеры цифровой подписи описаны в книгах B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, John Wiley & Sons, New York, 2nd edition, 1996 и A. J. Menezes, P. C. Van Oorschot, S. A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1997.

Электронные платежные системы, в которых неподделываемость платежных сертификатов обеспечивается цифровой подписью оператора платежной системы, делятся на офлайновые и онлайновые. В офлайновых платежных системах момент получения денег получателем платежа является момент успешной проверки получателем платежа платежных сертификатов, предоставленных плательщиком в качестве оплаты. Преимущество таких систем состоит в том, что передача денег от плательщика к получателю платежа может совершаться без участия третьей стороны. При этом защита

от многократного использования платежных сертификатов обеспечивается тем, что платежные сертификаты содержат в скрытой форме идентификатор плательщика, причем идентификатор плательщика, допустившего кратное использование, может быть раскрыт. Недостаток этого способа в том, что он не предотвращает многократное
5 использование платежных сертификатов, а позволяет лишь определить такое использование и возложить ответственность за него на определенного плательщика. Тем самым, в случае недоступности злоумышленника убытки понесет оператор платежной системы. Кроме того, может пострадать репутация добросовестного плательщика, информация о платежных сертификатах которого попала к злоумышленнику, и кото-
10 рый воспользовался таким сертификатом. Известно несколько офлайновых платежных систем. Например, одна такая система описана в патенте: Т. Okamoto, К. Ohta, Electronic cash system, U.S. Patent 5,224,162, 8 Jun 1992.

В онлайн-платежной системе получатель платежа обращается к оператору платежной системы для подтверждения каждого платежа. Многократное использование в
15 этом случае предотвращено тем, что оператор платежной системы хранит информацию о ранее использованных платежных сертификатах, а при проведении платежа с помощью некоторого платежного сертификата проверяет его неиспользованность.

Известен способ проведения платежей (Untraceable electronic cash, U.S. Patent 5,768,385, 16 Jun 1998), в котором плательщик получает в банке цифровые подписи
20 платежных сертификатов, называемых электронными монетами, которые он может использовать как для обмена на новые электронные монеты, так и для платежа. При этом банк не знает, в каком из этих двух режимов действует плательщик, что способствует непротраживаемости платежей. При этом защита от многократного использования электронных монет обеспечивается онлайн-проверкой получателем плате-
25 жа полученных электронных монет в банке. Однако известный способ не обеспечивает полной непротраживаемости такого участника системы, который в основном платит, а не получает платежи, так как электронные монеты, выданные такому участнику и предъявленные магазином для обмена, свидетельствуют, вообще говоря, о проведении платежа данным участником данному магазину.

Известен способ проведения платежей (D. Chaum, Security Without Identification: Transaction Systems to Make Big Brother Obsolete, Communications of the ACM, vol. 28 no. 10, October 1985 p. 1035-1038), который является наиболее близким аналогом к предлагаемому изобретению и выбран заявителем в качестве прототипа. В известном
30 способе клиент расплачивается платежными сертификатами, называемыми электронными монетами, подписи которых он получает в банке. При этом заранее фиксируется набор возможных номиналов, а для каждого возможного номинала электронной монеты банк создает секретный и открытый денежные ключи. Для получения электронной монеты плательщик выбирает ее номер посредством датчика случайных чисел и с по-
35 мощью процедуры изготовления вслепую цифровой подписи в банке, желающем про-
40 кредитовать плательщика на соответствующую сумму, получает в качестве подписи платежного сертификата цифровую подпись выбранного номера. При платеже плательщик передает получателю набор электронных монет, а получатель, проверив их правильность, пересылает полученные монеты в банк для зачисления на свой счет. Банк, проверив правильность электронных монет, зачисляет соответствующую сумму

на счет получателя платежа, если монеты не были использованы ранее. Для проверки использованности банк хранит список номеров использованных монет, причем, встроенные в номера монет сроки действия позволяют удалять из списка старые номера.

Недостатки известного способа состоят в том, что репутация банка не защищена от нечестных клиентов, а деньги клиента не защищены от нечестного банка, так как нечестный клиент, получив отказ банка признать уже использованный сертификат второй раз, может обвинить банк в нечестности. В свою очередь, нечестный банк, получив сертификат на проверку, может заявить, что этот сертификат уже предъявлялся ранее. Кроме того, банк вынужден хранить в оперативных базах данных информацию о каждом из использованных сертификатов, что приводит к быстрому росту баз данных банка и к необходимости введения временных ограничений на действие сертификатов. Помимо этого, в известном способе сумма платежа является целочисленной комбинацией номиналов монет, что либо ограничивает диапазон платежей, либо ведет к росту числа используемых при платежах монет, что ведет к росту баз данных в банке и замедлению платежей.

Известно устройство для проведения платежей (Т. Okamoto, K. Ohta, Method and apparatus for implementing electronic cash, U.S. Patent 4,977,595, 11 Dec 1990), выбранное заявителем в качестве прототипа.

Известное устройство состоит из платежного устройства, магазина и банка, соединенных посредством телекоммуникационных сетей, причем платежное устройство имеет средство для пополнения платежного устройства с использованием изготовления вслепую денежной подписи банка, а банк имеет средство для изготовления денежной подписи. Кроме того, магазин содержит средство для офлайн-проверки платежных сертификатов, а банк содержит устройство для выявления злоумышленника в случае кратного использования им обязательства банка. Недостаток известного устройства состоит в том, что оно не предотвращает многократное использование платежных сертификатов, а позволяет лишь определить такое использование и возложить ответственность за него на определенного плательщика. Другой недостаток известного устройства состоит в низкой скорости его работы, что вызвано большим размером передаваемых по коммуникационным сетям данных.

Раскрытие изобретения

Основной задачей, решаемой вариантами заявленного изобретения, является создание таких способов проведения платежей, которые обеспечили бы эффективный и надежный механизм расплаты по открытым коммуникационным сетям, защиту каждого участника платежной системы от злоупотреблений всех других участников, защиту приватности рядовых участников платежей, широкий диапазон платежей.

Единый для всех вариантов заявленного способа проведения платежей технический результат, состоит в том, что при проведении платежей по открытым телекоммуникационным сетям денежные интересы каждого участника защищены от злоупотреблений всех других участников, причем плательщики и получатели платежей имеют возможность защиты своей приватности. Помимо этого, в некоторых из заявленных вариантов, доступны платежи в диапазоне от микроплатежей до платежей бизнес-уровня, время проведения платежа зависит только от быстроты действия сетевых соединений, но не от суммы платежа, число клиентов, которые могут быть обслужены

оператором платежной системы, растет пропорционально его ресурсам. Способ проведения платежей реализуется устройством, конструируемым программными средствами.

5 Существенное отличие заявленного изобретения от известного уровня техники заключается в том, что помимо защиты приватности участников платежа обеспечена защита денежных интересов плательщика, поскольку платеж проводится на основании его платежного поручения, подписанного связанным с платежным сертификатом секретным ключом. Помимо этого, в некоторых из заявленных вариантов, допускается постепенное расходование платежных сертификатов и их пополнение.

10 Приватность плательщика защищена процедурой изготовления подписи платежного сертификата вслепую, а приватность получателя платежа может быть защищена тем, что при открытии счета получатель платежа не обязан сообщать сведений, идентифицирующих его личность. В тех вариантах, где оператор платежной системы контролирует условия платежа и, в частности, сведения о цели платежа, приватность плательщика и получателя платежа защищена тем, что такой контроль проводится без
15 доступа к конфиденциальной части условий платежа.

Заявленный способ проведения платежей предназначен исключительно для аппаратной или компьютерной реализации, так как обработка данных, используемых при проведении платежей, и, в частности, изготовление и проверка цифровых подписей
20 практически может быть реализована только на аппаратной или компьютерной основе.

Приведенное ниже описание способа проведения платежей предназначено для раскрытия изобретения и не ограничивает рамки заявленного изобретения, описанного более полно где-либо еще в настоящей заявке.

25 Ниже приведены сведения, уточняющие используемую в данной заявке терминологию.

При проведении платежей с использованием цифровой подписи, как и во всякой системе, использующих цифровую подпись, имеют дело с данными, которые располагаются на подходящих материальных носителях и могут быть представлены цифровым образом (B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, John Wiley&Sons, New York, 2nd edition, 1996 и A. J. Menezes, P. C. Van Oorshot, S. A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1997).

В некоторых схемах цифровой подписи легко получить цифровую подпись случайных данных без доступа к секретным ключам. Для избежания получения цифровой
35 подписи помимо воли владельца секретного ключа среди всех данных выделяют множество действительных данных, а в проверку правильности подписи для некоторых данных включает проверку действительности этих данных. Фиксация критерия действительности входит в понятие системы цифровой подписи. В частности, критерием действительности может быть совпадение части данных с заранее фиксированной последовательностью битов. В другом примере критерия действительности, данные считают действительными, если они представляет собой пару (X, Y), где $F(X)=Y$, а F
40 односторонняя функция (B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, John Wiley&Sons, New York, 2nd edition, 1996, p. 29-30 и A. J. Menezes, P. C. Van Oorshot, S. A. Vanstone, Handbook of Applied Cryptography, CRC

Press, 1997, p. 8-9), то есть, в данном случае, такая функция, которая вычислительно необратима для всех, кроме, возможно, подписывающей стороны.

Ниже ключи для подписи называются просто ключами, а назначение ключей, используемых для иных целей, уточняется.

- 5 Под оператором платежной системы имеется в виду сторона, обеспечивающая проведение расчетов участников платежей. В частности оператор платежной системы может вести счета участников платежей и эмитировать ценные документы. Оператор платежной системы может состоять из одного банка, а может включать в себя несколько организаций, в том числе и банков, которые связаны между собой различными
10 договорными обязательствами. В частности, секретные ключи оператора платежной системы могут быть секретом одной из организаций, входящих в состав оператора платежной системы, а обязательства оператора платежной системы перед третьей стороной также могут быть обязательствами лишь одной из организаций, входящих в состав оператора платежной системы. В том случае, когда оператор платежной системы
15 включает несколько различных банков или иных организаций, должна иметься безопасная система урегулирования взаимных обязательств между организациями, входящими в состав оператора платежной системы. Для упрощения текста заявки далее вместо термина "оператор платежной системы" используется термин "оператор".

- 20 Под платежным сервером имеется в виду устройство, при помощи которого оператор обслуживает проведение платежей. Такой платежный сервер может состоять как из одного, так и из нескольких компьютеров, или иных устройств.

Под платежным устройством имеется в виду устройство, при помощи которого проводит платежи плательщик, а под приемным устройством имеется в виду устройство, при помощи которого проводит платежи получатель платежа.

- 25 Под платежным сертификатом имеются в виду цифровые данные, представляющие обязательство оператора. Платежный сертификат включает основу, подпись и уровень.

- 30 Под основой платежного сертификата имеются в виду данные, подпись для которых, проверенная денежным открытым ключом, служит подтверждением обязательств оператора по этому сертификату и называется подписью платежного сертификата. Подпись платежного сертификата изготавливают денежным секретным ключом оператора, соответствующим используемому для проверки этой подписи денежному открытому ключу. Далее вместо термина "денежный секретный ключ оператора" используется термин "денежный секретный ключ".

- 35 Понятие уровня платежного сертификата основано на понятии уровня денежных открытого и секретного ключей. Под уровнем открытого денежного ключа имеется в виду сопоставленная этому открытому денежному ключу численная характеристика, определяющая некоторую денежную ценность. Уровень может быть представлен как
40 одним, так и несколькими числами. Например, уровень может быть представлен неотрицательным целым числом L , выражающем в центах денежную ценность, определяемую этим уровнем. В другом примере, уровень может быть представлен набором неотрицательных целых чисел $L = (L_1, \dots, L_k)$, а выраженная в центах денежная ценность определяется этим уровнем по формуле $L_1 \cdot N_1 + \dots + L_k \cdot N_k$, где N_1, \dots, N_k заранее фиксированные целые неотрицательные числа. В этом случае числа L_j называют раз-

рядами, а превышение одного уровня над другим определяют поразрядно. Под уровнем секретного денежного ключа имеется в виду уровень соответствующего открытого денежного ключа, а под уровнем платежного сертификата имеется в виду уровень подписи платежного сертификата, то есть уровень того открытого денежного ключа, которым может быть проверена эта подпись.

Ниже дано описание способа проведения платежей по первому варианту.

Проведение платежа включает проведение операции пополнения платежного устройства, операции открытия счета получателя платежа и собственно платежной операции.

Пополнение платежного устройства осуществляют получением с помощью платежного сервера подписи платежного сертификата. При этом подпись платежного сертификата получают посредством изготовления вслепую денежной подписи оператора, что ведет к несвязываемости платежного сертификата с источником пополнения и, тем самым, к обеспечению приватности плательщика.

Пополнение платежного устройства осуществляют посредством операции первичного наполнения платежного сертификата, при которой в платежном устройстве создают основу платежного сертификата и получают с помощью платежного сервера подпись платежного сертификата. Ниже приведено отдельное описание операции создания основы платежного сертификата.

Основу платежного сертификата создают в платежном устройстве. Для создания основы *Base* платежного сертификата выбирают произвольный секретный ключ плательщика *DP* и соответствующий ему открытый ключ *EP*. Такой выбор осуществляют в рамках произвольной системы цифровой подписи. Выбранные ключи *DP* и *EP* принимают в качестве секретного и, соответственно, открытого ключа платежного сертификата. В основу *Base* платежного сертификата включают идентификатор открытого ключа *EP*. Под идентификатором открытого ключа имеются в виду произвольные данные, которые однозначно определяют открытый ключ. В качестве такого идентификатора, в частности, может быть взят сам открытый ключ *EP*. В другом примере, идентификатором может служить значение односторонней хэш-функции (B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, John Wiley&Sons, New York, 2nd edition, 1996, p. 429) на ключе *EP*. Еще в одном примере, идентификатором может быть номер открытого ключа, полученный при его регистрации у оператора или иной стороны.

Включение в основу *Base* платежного сертификата идентификатора открытого ключа *EP*, позволяет обезопасить плательщика при проведении платежа. А именно, при проведении платежной операции, как это описано ниже, оператор может израсходовать связанные с платежным сертификатом ценности лишь в соответствии с подписанным платежным поручением плательщика. Подпись платежного поручения плательщика изготавливают секретным ключом *DP*, а проверяют эту подпись открытым ключом *EP*. Поскольку секретный ключ *DP* доступен только плательщику, то и такую подпись невозможно получить помимо воли плательщика.

В частности, включение идентификатора открытого ключа *EP* в основу *Base* платежного сертификата осуществляют следующим образом. В качестве основы используют пары (X, Y) , где $X = EP$, $Y = F(X)$, а F односторонняя функция, которая, предпоч-

тительно, кроме того, обладает свойством "collision free" (B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, John Wiley&Sons, New York, 2nd edition, 1996, p. 30). В этом случае в качестве идентификатора основы при проведении операций с платежным сертификатом могут быть использованы данные Y , а равенство $Y = F(X)$ используют в качестве критерия действительности основы, где под критерием действительности основы платежного сертификата имеется в виду критерий действительности системы подписи, к которой относятся денежные ключи.

Ниже приведено отдельное описание получения подписи платежного сертификата посредством изготовления вслепую денежной подписи оператора при первичном наполнении платежного сертификата.

При операции первичного наполнения платежного сертификата с основой *Base* подпись платежного сертификата получают посредством процедуры изготовления вслепую цифровой подписи оператора в рамках произвольной системы цифровой подписи, допускающей изготовление цифровой подписи вслепую.

Известно несколько систем цифровой подписи, допускающей изготовление цифровой подписи вслепую (D. Chaum, Blind Signature Systems, U.S. Patent 4,759,063, 19 Jul 1988; D. Chaum, Blind Unanticipated Signature Systems, U.S. Patent 4,759,064, 19 Jul 1988; D. Pointcheval, J. Stern, Provably Secure Blind Signature, Lectures Notes in Computer Science, 1163, 1996, Springer, p. 252-265, и другие). При изготовлении вслепую цифровой подписи для исходных данных M пользователь предоставляет подписывающей стороне замаскированные данные M' , полученные маскировкой данных M . Подписывающая сторона предоставляет пользователю данные для демаскировки S' , полученные обработкой замаскированных данных M' секретным ключом подписывающей стороны, а пользователь получает подпись S исходного сообщения посредством демаскировки. Свойство подписи для данных, полученных в результате демаскировки, может быть проверено не только после демаскировки, но и до демаскировки, если используемая система цифровой подписи допускает это.

При проведении операции первичного наполнения платежного сертификата в качестве исходных данных берут идентификатор *BaseId* основы платежного сертификата, то есть произвольные данные, идентифицирующая эту основу. Обработку замаскированных данных при получении подписи платежного сертификата посредством процедуры изготовления цифровой подписи вслепую производят денежным секретным ключом, соответствующим сумме пополнения, причем под соответствием суммы пополнения и денежного секретного ключа имеется в виду соответствие суммы пополнения и денежной ценности, определяемой уровнем этого денежного секретного ключа.

Подпись идентификатора *BaseId*, полученную посредством демаскировки полученных из платежного сервера данных для демаскировки, принимают в качестве подписи платежного сертификата с основой *Base*. Правильность изготовленной подписи платежного сертификата может быть проверена открытым денежным ключом, соответствующим использованному при изготовлении данных для демаскировки секретному денежному ключу.

Таким образом, после проведения операции первичного наполнения платежного сертификата в платежном устройстве имеется годный для проведения платежной опе-

рации платежный сертификат.

При проведении операции первичного наполнения платежного сертификата замаскированный идентификатор основы доставляют в платежный сервер как часть формируемого в платежном устройстве денежного запроса, а пополнения платежно-
5 го устройства осуществляют из средств источника пополнения, указанного в этом денежном запросе. При этом с точки зрения оператора, источник пополнения платежного устройства, является источником кредитования, так в итоге операции пополнения в платежном устройстве оказывается денежное обязательство оператора, а плательщик, таким образом, оказывается прокредитованным. Кроме источника по-
10 полнения по денежному запросу определяют и сумму пополнения, если она не предусмотрена иными обстоятельствами, например условиями обслуживания указанного источника пополнения.

В качестве источника пополнения указывают, в частности, счет плательщика или его банковскую карточку, где под банковской карточкой имеется в виду произвольная ценная карточка, предназначенная для проведения платежей. Безопасность удаленного востребования ценностей с указанного источника пополнения обеспечивают системой обслуживания этого источника.

Операция открытия счета плательщика у оператора может быть осуществлена произвольным способом. Предпочтительно, чтобы открываемый счет допускал
20 безопасную систему удаленного управления.

Примером счета, допускающего безопасную систему удаленного управления, является счет с открытым ключом. Под счетом с открытым ключом имеется в виду счет, хранимый у оператора и допускающий управление подписанными приказами, подпись для которых может быть проверена связанным со счетом открытым ключом. Для
25 управления таким счетом его владелец может использовать свой секретный ключ, соответствующий открытому ключу счета и называемый секретным ключом счета. Безопасность удаленного управления счетом с открытым ключом обеспечивают тем, что оператор проводит операции с данным счетом, руководствуясь подписанными указаниями, подпись для которых проверяют открытым ключом счета и которые используют для отчетности оператора перед владельцем счета.
30

Счет с открытым ключом помимо управления посредством указаний, подписанных секретным ключом счета, может предусматривать и другие способы управления. В частности, с таким счетом может быть связана информация, идентифицирующая распорядителя счета, то есть субъекта, имеющего право управлять счетом. Такая информация может быть особенно полезной в случае утраты секретного ключа счета, так как
35 позволит владельцу и в этом случае сохранить контроль над своим счетом.

Более того, если требуется обеспечить анонимность распорядителя счета, то идентифицирующая распорядителя информация может находиться в платежном сервере в скрытой форме, то не позволяющей связать эту информацию с распорядителем по-
40 мимо его воли того, кому эта связь известна. Например, в качестве такой скрытой информации можно использовать образ односторонней хэш-функции от паспортных данных распорядителя, объединенных с паролем, или просто от пароля. Связывание со счетом идентифицирующей распорядителя счета информации может быть осуществлено по подписанному секретным ключом счета указанию, как при открытии счета,

так и в другие моменты времени.

Ниже приведено отдельное описание частного случая операции открытия счета с открытым ключом. Это описание будет использовано далее для ссылок при описании других вариантов заявленного изобретения. В частности описанная ниже операция

5 открытия счета может быть использована как при открытии счета получателя платежа, так и счета плательщика, а открытый таким образом счет плательщика может быть использован в качестве источника пополнения платежного устройства.

Операция открытия счета с открытым ключом, в частности, может происходить следующим образом. Будущий владелец открываемого счета, в качестве секретного

10 ключа счета принимает свой произвольный секретный ключ. Открытый ключ, соответствующий секретному ключу счета доставляют в платежный сервер и принимают в качестве открытого ключа открываемого счета. Владелец счета считает счет открытым после получения подписанного оператором сообщения, которое подтверждает открытие счета, связанного с открытым ключом счета.

Помимо открытого ключа счета с открываемым счетом могут быть связаны и иные данные, выбранные как владельцем, так и оператором. Например, оператор может присвоить открываемому счету номер, который сообщается владельцу счета. Предпочтительно, чтобы данные, связываемые со счетом его владельцем, носили заявительный характер, что обеспечивает автоматическое проведение и, тем самым, деше-

15 визну операции открытия счета и его обслуживания. Приватность владельца счета может быть защищена тем, что счет открывают анонимным образом.

Ниже приведено отдельное описание платежной операции по первому варианту. На это описание ниже будут даны ссылки при описании других вариантов заявленного изобретения. При проведении платежной операции по первому варианту заключенная

25 в платежном сертификате стоимость расходуется полностью. Так как в других вариантах заявленного изобретения, кроме таких платежных операций, проводят и платежные операции, допускающее постепенное расходование заключенной в платежном сертификате стоимости, то, для большей определенности, используемая в данном варианте платежная операция, описана как платежная операция с погашением платежного сертификата.

30

Сущность платежной операции с погашением платежного сертификата состоит в том, что в платежном сервере осуществляют кредитование счета получателя платежа, аннулируя при этом обязательство оператора по платежному сертификату. Кредитование счета получателя платежа осуществляют в случае неиспользованности платежного сертификата, правильности подписи платежного сертификата и правильности подписи для платежного поручения плательщика. Об использованности платежного сертификата судят по содержащейся в информационном хранилище платежного сервера информации об использованных платежных сертификатах, а подпись платежного сертификата и подписанное секретным ключом платежного сертификата платежное

35 поручение плательщика доставляют в платежный сервер посредством приемного устройства. Более детальное описание платежной операции с погашением платежного сертификата состоит в следующем.

40

При проведении платежной операции в платежном устройстве формируют платежное поручение плательщика, в которое включают сведения о получателе платежа и

идентификатор основы платежного сертификата. Платежное поручение плательщика, подписанное секретным ключом платежного сертификата, включает в данные, доставляемые в приемное устройство и называемые платежными данными. В качестве сведений о получателе платежа в платежное поручение плательщика, в частности, включают идентификатор счета получателя платежа, если этот счет не определен иными обстоятельствами, и условия платежа.

Под условиями платежа имеются в виду произвольные данные, уточняющие обстоятельства проведения платежа. К таким данным, в частности, относятся сумма платежа и ограничения на время проведения платежа. В частности, условия платежа могут содержать, возможно, в скрытой от оператора форме, обязательства, накладываемые на получателя платежа фактом его проведения.

В приемном устройстве формируют данные, называемые платежным поручением получателя платежа, которые доставляют в платежный сервер. При этом в платежное поручение получателя платежа включают платежное поручение плательщика, содержащееся в платежных данных и, возможно, иные данные, к которым, в частности, относятся условия платежа. Кроме того, платежное поручение плательщика может быть подписано секретным ключом счета получателя платежа, если счет плательщика является счетом с открытым ключом.

В платежном сервере осуществляют кредитование счета получателя платежа на основе его платежного поручения и формируют ответ оператора на платежное поручение получателя платежа, по которому судят о проведении платежа. При этом кредитование счета получателя платежа осуществляют по отсутствию в информационном хранилище платежного сервера информации об использованности платежного сертификата. Кроме того, в платежном сервере до кредитования счета получателя платежа осуществляют проверку правильности подписи платежного сертификата и правильности подписи для платежного поручения плательщика, причем эти подписи берут из платежного поручения плательщика, содержащегося в полученном из приемного устройства платежном поручении получателя платежа. Для предотвращения повторного использования платежного сертификата информацию о нем заносят в информационное хранилище платежного сервера. Для подтверждения права оператора на совершение проводимой платежной операции в информационное хранилище платежного сервера также заносят подписанное платежное поручение плательщика. Ответ оператора на платежное поручение доставляют в приемное устройство.

Денежные интересы плательщика при проведении платежной операции защищены обязанностью оператора проверять подпись платежного поручения плательщика, а оператор защищен от напрасных обвинений в присвоении заключенной в платежном сертификате стоимости хранящимся в информационном хранилище подписанным платежным поручением плательщика.

Защиту приватности плательщика обеспечивают, в частности, тем, что платежное поручение плательщика, предназначенное для доставки в платежный сервер, шифруют шифровальным ключом оператора, где под шифровальным ключом некоторого субъекта имеется в виду ключ для шифрования предназначенное для этого субъекта сообщений.

Помимо платежного поручения плательщика, платежные данные, могут включать

данные, предназначенные для получателя платежа, и, в частности, идентификатор оплачиваемой услуги или товара.

В частности, безопасность получателя платежа обеспечивают тем, что в ответ оператора на платежное поручение получателя платежа, доставляемый получателю платежа, включают подписанную секретным ключом оператора квитанцию получателя платежа. При этом под квитанцией получателя платежа имеются в виду данные, подтверждающие факт кредитования счета получателя платежа. Такая квитанция, помимо суммы кредитования и идентификатора прокредитованного счета, может содержать и другие данные, в частности, условия платежа, время проведения операции кредитования и т.п. Получатель платежа, проверив правильность подписи оператора для квитанции получателя платежа, считает платеж проведенным, и доставляет плательщику данные, подтверждающие проведение платежа.

Более того, при проведении платежной операции в приемном устройстве по ответу оператора на платежное поручение получателя платежа, формируют и доставляют в платежное устройство данные, по которым судят о проведении платежа для плательщика. Эти данные могут содержать, в частности, как согласие получателя платежа с фактом завершенности платежной операции для получателя платежа, так и квитанцию плательщика, подписанную произвольным секретным ключом оператора. Такую квитанцию в платежном сервере включают в ответ оператора на платежное поручение получателя платежа, доставляемый получателю платежа, а в приемном устройстве берут из полученного ответа оператора на платежное поручение получателя платежа. При этом под квитанцией плательщика имеются в виду данные, подтверждающие факт расходования заключенной в платежном сертификате стоимости при проведении платежной операции. Помимо этого квитанция плательщика может содержать иные данные и, в частности, условия платежа и время проведения платежа оператором. Кроме того, перед включением в ответ оператора на платежное поручение получателя платежа квитанция плательщика может быть зашифрована произвольным шифровальным ключом плательщика. Более того, совместно с данными, по которым судят о проведении платежа для плательщика, в платежное устройство могут быть доставлены данные, связанные с выполнением получателем платежа своих обязательств, вытекающих из факта проведения платежа, и, в частности, пароль доступа к некоторой информации.

Стоимость, заключенная в платежном сертификате, может быть израсходована при платежной операции как полностью на цели платежа, так и частично на другие цели. В частности, часть стоимости платежного сертификата может быть возвращена в платежное устройство в качестве сдачи. Ниже приведено отдельное описание такой операции.

При возвращении части стоимости платежного сертификата платежное устройство пополняют как посредством первичного наполнения платежного сертификата, так и пополнением уже имеющегося платежного сертификата. Более того, возвращение остатка платежного сертификата, то есть неизрасходованной части заключенной в платежном сертификате стоимости, может быть осуществлено таким образом, что возвращаемый остаток останется неизвестным оператору. Такое возвращение остатка может быть осуществлено, например, с помощью способа, описанного в патенте:

David Chaum, Returned value blind signature systems, U.S. Patent 4 949 380, 14 Aug 1990. В лучшем варианте реализации операции возвращения части стоимости платежного сертификата в платежное устройство первичное наполнение платежного сертификата неотлично для оператора от пополнения уже имеющегося платежного сертификата,

5 что способствует защите приватности плательщика.

Безопасность получателя платежа при проведении платежной операции обеспечивают, в частности, тем, что в ответ оператора на платежное поручение получателя платежа включают квитанцию получателя платежа, подписанную произвольным секретным ключом оператора, а о проведении платежа для получателя платежа судят по
10 правильности подписи для квитанции получателя платежа.

Помимо этого, плательщик может контролировать обстоятельства проведения платежной операции. Для такого контроля при формировании платежного поручения плательщика в него включают условия платежа. В частности, в условия платежа, содержащиеся в платежном поручении плательщика, могут быть включены данные обязательства получателя платежа по платежу. Для того, чтобы плательщик в случае не-
15 необходимости мог настоять на выполнении получателем платежа его обязательств, данные обязательства получателя платежа по платежу подписывают произвольным секретным ключом получателя платежа, а перед принятием решения плательщика о проведении платежной операции в платежном устройстве проверяют правильность
20 подписи для данных обязательства получателя платежа по платежу и сохраняют подписанные данные обязательства получателя платежа по платежу. Для того, чтобы скрыть цель платежа от оператора, в платежном устройстве при формировании платежных данных производят обработку данных обязательства получателя платежа по платежу произвольной односторонней функцией, причем данные, полученные при
25 этой обработке, включают в платежное поручение получателя платежа в качестве условий платежа.

Кроме того, при проведении платежной операции в качестве плательщика может выступать получатель платежа. Такую платежную операцию можно использовать для перевода ценностей из платежного устройства на счет плательщика.

30 Отметим частный случай осуществления операции пополнения платежного устройства, в котором пополнение производят из средств промежуточного плательщика. В частности, при таком проведении пополнения платежного устройства замаскированные в платежном устройстве данные при изготовлении вслепую денежной подписи оператора подвергают дополнительной маскировке в платежном устройстве промежу-
35 точного плательщика, а полученные от оператора данные для демаскировки подвергают соответствующей дополнительной демаскировке. Дополнительная маскировка предназначена для защиты приватности промежуточного плательщика.

Общая проблема всех электронных систем массового обслуживания, заботящихся о приватности пользователей, состоит в возможности определения личности пользова-
40 теля по сетевой адресной информации. Несколько теоретических подходов к решению этой проблемы описано в статье D. Chaum, Security Without Identification: Transaction Systems to Make Big Brother Obsolete, Communications of the ACM, vol. 28 no. 10, October 1985 p. 1031-1034. Практически приемлемым способом сокрытия сетевой адресной информации пользователя от адресата сообщения может быть использование

посредников, передающих сообщение адресату со своего адреса. В частности, во всех вариантах заявленного изобретения при проведении платежной операции сокрытие адреса плательщика от банка частично достигается тем, что платежное поручение плательщика доставляют в платежный сервер через приемное устройство получателя платежа.

В некоторых вариантах реализации способа проведения платежей по первому варианту доступны платежи в диапазоне от микроплатежей до платежей бизнес-уровня, а время проведения платежа зависит только от скорости действия сетевых соединений, но не от суммы платежа, что достигается таким выбором уровней платежных сертификатов, при котором определяемая уровнем ценность может принимать произвольные значения в указанном диапазоне, и проведением платежной операции с использованием заранее ограниченного количества платежных сертификатов подходящей стоимости, или даже единственного платежного сертификата.

Ниже дано описание способа проведения платежей по второму варианту.

Проведение платежей по второму варианту осуществляют так же, как и по первому варианту, за исключением того, что помимо пополнения платежного устройства посредством первичного наполнения платежного сертификата, проводят также пополнение платежного устройства пополнением платежного сертификата. При этом в лучшем варианте реализации при пополнении платежного устройства первичное наполнение платежного сертификата неотличимо для оператора от пополнения уже имеющегося платежного сертификата, а источник средств для такого пополнения не связан с источником средств для первичного наполнения.

При проведении платежной операции по первому варианту в случае предъявления в платежный сервер подписи платежного сертификата максимально доступного в платежном устройстве уровня оператор может обнаружить совпадение этого уровня с уровнем денежных ключей, использованных при пополнении платежного устройства, что может привести к связыванию используемого при платеже платежного сертификата с источником его пополнения. Вероятность этого особенно велика в том случае, когда возможные уровни платежных сертификатов таковы, что определяемая уровнем ценность может принимать произвольные значения в диапазоне от микроплатежей до платежей бизнес-уровня. Пополнение платежного устройства пополнением платежного сертификата значительно уменьшает возможность такого связывания, так как уровень платежного сертификата после его пополнения является суммой нескольких уровней подписей денежными секретными ключами. Тем самым пополнение платежного сертификата дополнительно способствует защите приватности плательщика. Кроме того, пополнение платежного сертификата дополнительно позволяет как накапливать возвращенные при платежных операциях остатки использованных платежных сертификатов на одном платежном сертификате, так и пополнять этот платежный сертификат из средств иного источника.

Ниже приведено отдельное описание операции пополнения платежного устройства посредством пополнения платежного сертификата.

Операцию пополнения платежного сертификата, то есть операцию получения подписи платежного сертификата, уровень которой превышает уровень той подписи платежного сертификата, которая имеется в платежном устройстве к началу операции

- пополнения, осуществляют посредством изготовления вслепую денежной подписи оператора. При этом в качестве исходных данных берут имеющуюся в платежном устройстве подпись платежного сертификата. Для проведения операции пополнения платежного сертификата соответствие уровней и денежных ключей должно быть та-
- 5 ким, что подпись уровня A для некоторых данных X , в качестве которых взята подпись уровня B для некоторых данных Y , соответствует подписи уровня $(A + B)$ для данных Y . В качестве примера такого соответствия приведем случай, когда уровень L представлен набором неотрицательных целых чисел (L_1, L_2, \dots, L_k) , а для каждого индекса j от 1 до k имеется функция S_j , для вычисления которой необходим секретный ключ K_j .
- 10 В том случае, когда функции S_j перестановочны друг с другом, то есть $S_j(S_i(X)) = S_i(S_j(X))$ для произвольных данных X , в качестве денежного ключа, соответствующего уровню L , могут быть взяты произвольные данные, позволяющие вычислять функцию S_L , являющуюся композицией функций S_j , каждая из которых входит в композицию с кратностью L_j . В этом случае подписью данных X денежным ключом, соответствующим
- 15 уровню L , являются данные $S_L(X)$. Например, такой ключ может быть представлен набором данных $(L, K_1, K_2, \dots, K_k)$. Пример конкретной системы таких функций, допускающий экономное изготовление и хранение секретных ключей приведен далее при описании лучшего варианта реализации способа проведения платежей. Отметим, что операция напoлнения платежного сертификата является частным случаем опера-
- 20 ции пополнения платежного сертификата, если идентификатор основы платежного сертификата принять в качестве подписи нулевого уровня.

В лучшем варианте реализации операции пополнения платежных сертификатов путем увеличения их уровня с помощью оператора, изготавливающего вслепую подпись платежного сертификата повышенного уровня, оператор не имеет возможности опре-

25 делить, осуществляет ли плательщик пополнение уже имеющегося платежного сертификата, или они служат для напoлнения вновь созданного платежного сертификата. При этом при пополнении одного и того же платежного сертификата плательщик может использовать различные источники пополнения, не связывая их между собой.

Ниже дано описание способа проведения платежей по третьему варианту.

- 30 Проведение платежей по третьему варианту осуществляют так же, как и по первому варианту, за исключением того, что используют многоразовые платежные сертификаты. Это выражается в том, что оператор открывает связанный с данным платежным сертификатом платежный счет и связывает его с открытым ключом подписи платежного сертификата. При этом кредитование счета получателя платежа при проведении
- 35 платежной операции осуществляют за счет средств платежного счета, кредитование которого осуществляют за счет платежного сертификата. Тем самым возможно постепенное расходование заключенной в платежном сертификате стоимости.

Под платежным счетом имеется в виду счет у оператора, допускающий проведение с него платежей путем перевода части суммы счета на другой счет или перевода части

40 суммы счета в иную форму для выдачи их получателю платежа. При этом платежный счет содержит информацию о суммарной величине расходов, информацию о суммарной величине поступлений на этот счет и информацию об уровне платежного счета. При этом под уровнем платежного счета имеются в виду уровень предъявленной оператору для кредитования платежного счета подписи платежного сертификата. В част-

ности, в качестве платежного счета возможно использование счета с открытым ключом.

Ниже приведено отдельное описание операции открытия платежного счета.

Для открытия платежного счета, связанного с основной платежным сертификатом, достаточно доставить в платежный сервер идентификатор основы этого платежного сертификата. В частности, открытие платежного счета может быть совмещено с первой платежной операцией, связанной с платежным сертификатом. В том случае, когда в качестве платежного счета используют счет с открытым ключом, в качестве этого ключа возможно использовать открытый ключ платежного сертификата. Более того, для предохранения платежного сервера от открытия таких платежных счетов, которые не связаны с платежным сертификатом положительного уровня, операция открытия счета может быть совмещена с операцией его кредитования.

Ниже приведено отдельное описание операции кредитования платежного счета.

При операции кредитования платежного счета в платежный сервер доставляют подпись платежного сертификата, уровень которой выбирают произвольно в пределах уровня платежного сертификата, а кредитование платежного счета осуществляют в соответствии с превышением уровня доставленной подписи над уровнем платежного счета. В частности, операция кредитования платежного счета может быть совмещена с платежной операцией. Кроме того, плательщик может кредитовать свой платежный счет в ходе нескольких операций, шаг за шагом повышая известный оператору уровень платежного сертификата. Это позволяет плательщику ослабить возможность связывания с помощью уровня платежного сертификата платежного счета и источников наполнения или пополнения связанного с этим счетом платежного сертификата.

Ниже приведено отдельное описание используемой в способе проведения платежей по третьему варианту платежной операции. В отличие от ранее описанной платежной операции с погашением платежного сертификата используемая в способе проведения платежей по третьему варианту платежная операция описана как платежная операция с использованием платежного счета.

Платежную операцию с использованием платежного счета проводят также как и вышеописанную платежную операцию с погашением платежного сертификата за исключением следующего. Во-первых, кредитование счета получателя платежа осуществляют из средств платежного счета, а, во-вторых, в платежное поручение плательщика не обязательно включают подпись платежного сертификата. При этом действия получателя платежа не отличаются от его действий при проведении платежной операции с погашением платежного сертификата.

При проведении платежной операции с погашением платежного сертификата имеются проблемы с диапазоном платежей. Дело в том, что заключенная в платежном сертификате стоимость может принимать лишь значения, соответствующие одному из возможных уровней платежных сертификатов или, что то же самое, одному из возможных уровней денежных ключей. Тем самым, если при проведении платежной операции с погашением платежного сертификата используется лишь один платежный сертификат, то величина платежа может принимать лишь одно из заранее определенных значений. Необходимости проводить платежи в диапазоне от платежей бизнес-уровня до микроплатежей ведет к тому, что либо приходится иметь достаточно раз-

ветвленную систему денежных ключей, либо использовать при платежной операции наборы платежных сертификатов. Применение разветвленной системы денежных ключей, вообще говоря, ведет к замедлению платежных операций, так как изготовление денежной подписи и проверка ее правильности требуют значительного времени.

- 5 Использование же при платежной операции наборов платежных сертификатов ведет как к значительному росту числа используемых платежных сертификатов со всеми вытекающими отсюда издержками, так и к неудобствам для плательщика, вынужденного обеспечивать наличие в платежном устройстве наборов необходимой суммарной стоимости. Преимущества платежной операции с использованием платежного счета
- 10 состоят в том, что проблемы с диапазоном платежей отсутствуют, так как величина платежа не связана со структурой уровней денежных ключей. Поэтому использование платежных счетов позволяет провести платеж на произвольную сумму в пределах платежеспособности платежного счета и, в частности, возможно проведение микроплатежей. Для оператора преимущество использования платежных счетов состоит в
- 15 том, что он может обслужить потенциально гораздо большее число клиентов, так как не требуется ресурсов для хранения информации о каждом проведенном платеже. К тому же, существенно меньшее число связанных с платежными сертификатами записей ускоряет при проведении платежной операции поиск записи, связанной с конкретным платежным сертификатом, или выяснение отсутствия такой записи. Недостаток
- 20 использования платежных счетов состоит в возможности связывания всех платежей проведенных с использованием одного и того же платежного счета. Тем самым, максимальное число используемых одновременно платежных сертификатов пропорционально ресурсам оператора. А так как пропорциональность числа используемых платежных сертификатов числу клиентов оператора может быть ограничена как стоимостью операции открытия платежного счета, так и стоимостью операции изготовления
- 25 вслепую денежной подписи, то и число клиентов, которые могут быть обслужены оператором, пропорционально ресурсам оператора.

Еще одно преимущество проведения платежной операции с использованием платежного сертификата по сравнению с такой платежной операцией с погашением платежного сертификата, при которой используют набором платежных сертификатов, состоит в том, что время проведения платежа зависит только от быстроты действия сетевых соединений, но не от суммы платежа, так как фиксированный размер платежного поручения плательщика допускает указание любой практически возможной суммы в качестве суммы платежа.

- 35 Кроме того, платежный счет, связанный с одним из платежных сертификатов может быть использован при операции пополнения платежного устройства в качестве источника пополнения. Тем самым может быть осуществлен перевод средств с платежного счета в платежное устройство.

Ниже дано описание способа проведения платежей по четвертому варианту.

- 40 Проведение платежей по четвертому варианту осуществляют так же, как и по третьему варианту, за исключением того, что, как и в вышеописанном способе проведения платежей по второму варианту, дополнительно проводят операцию пополнения платежного сертификата. Дополнительные преимущества проведению такой операции также указаны в вышеприведенном описании способа проведения платежей по второ-

му варианту.

Ниже дано описание устройства для проведения платежей. Посредством этого устройства возможна реализация третьего и четвертого вариантов заявленного способа проведения платежей.

- 5 Устройство для проведения платежей содержит платежное устройство, приемное устройство и платежный сервер, соединенные телекоммуникационными сетями. Каждое из этих устройств может быть реализовано вычислительным устройством, которое запрограммировано соответствующим образом.

- 10 Такое вычислительное устройство может быть выбрано из большого многообразия известных электронных устройств, таких, например, как персональные компьютеры. Такие вычислительные устройства включают, внутренним или внешним образом, запоминающие устройства, которые требуются для хранения данных или кодов программ, вовлеченных в проведение платежа. Кроме того, такие вычислительные устройства включают вспомогательные устройства, например, модемы, которые делают
15 вычислительные устройства способными общаться с другими подобными устройствами. Коммуникационная среда, в рамках которой производят обмен данными, также может быть произвольной из большого числа возможностей, включающих телефонные линии, кабели, Интернет, передающие спутники, радиосвязь, оптоволоконную связь и т.п. Иными словами, не предполагается, что изобретение ограничено по отношению к тем или иным типам используемых устройств и средств их коммуникации.
20

- Платежное устройство, приемное устройство и платежный сервер могут быть реализованы большим многообразием программных средств, основанных на соответствующих алгоритмах. При этом платежное устройство содержит средство для пополнения платежного устройства с использованием изготовления вслепую денежной подписи оператора, средство для создания основы платежного сертификата обработкой
25 односторонней функцией открытого ключа платежного сертификата, средство для сохранения созданной основы платежного сертификата в запоминающем устройстве и средство для формирования платежного поручения плательщика, подписанного секретным ключом платежного сертификата. При этом средство для пополнения платежного устройства с использованием изготовления вслепую денежной подписи оператора реализовано средством для повышения уровня подписи платежного сертификата.
30

- Это средство для повышения уровня подписи платежного сертификата имеет средство формирования денежного запроса, включающего замаскированную подпись платежного сертификата, средство для демаскировки содержащихся в ответе на денежный запрос данных для демаскировки и средство для занесения результата демаскировки в упомянутое запоминающее устройство.
35

- Средство для повышения уровня подписи платежного сертификата предназначено для пополнения платежного устройства, как первоначальным наполнением платежного сертификата, так и пополнением платежного сертификата. В первом случае с помощью средства для повышения уровня подписи платежного сертификата обрабатывается подпись нулевого уровня платежного сертификата, в качестве которой используется идентификатор основы платежного сертификата, созданной при помощи упомянутого выше средства для создания основы платежного сертификата. Во втором случае, с помощью средства для повышения уровня подписи платежного сертификата
40

обрабатывается имеющаяся в платежном устройстве подпись платежного сертификата, которая занесена в запоминающее устройство платежного устройства при одной из предшествующих операций пополнения платежного устройства. В обоих случаях в итоге пополнения платежного устройства происходит повышение уровня платежного сертификата.

Приемное устройство содержит средство для формирования платежного поручения получателя платежа, включающего платежное поручение плательщика. Кроме того, приемное устройство содержит средство для открытия счета с открытым ключом.

Платежный сервер содержит средство для изготовления денежной подписи, средство для проведения платежной операции, средство для обслуживания базы данных платежных счетов и средство для обслуживания базы данных счетов.

При этом под средством обслуживания произвольной базы данных имеется в виду средство для осуществления операций с записями этой базы данных, в том числе для создания таких записей, для их считывания и модификации.

Средство для обслуживания базы данных счетов может иметь, кроме того, средства, предназначенные для обслуживания счетов, которые представляют собой записи в этой базе данных и хранятся в запоминающем устройстве. К таким средствам относятся, в частности, средство для открытия счета с открытым ключом, средство для кредитования счета и средство для списывания со счета средств.

Средство для обслуживания базы данных платежных счетов может иметь, кроме того, средства, предназначенные для обслуживания платежных счетов, которые представляют собой записи в этой базе данных и хранятся в запоминающем устройстве. К таким средствам относятся, в частности, средство для открытия платежного счета, средство для проверки денежной подписи и средство для кредитования платежного счета.

Кроме того, имеющееся в платежном сервере средство для проведения платежной операции имеет средство для проверки подписи платежного поручения плательщика и средство для изготовления подписанной квитанции получателя платежа,

Упомянутое средство для изготовления денежной подписи используется имеющимся в платежном сервере средством для обработки денежного запроса при выполнении операции пополнения платежного устройства.

Кроме того, платежный сервер может содержать средство для изготовления подписанной квитанции получателя платежа, а приемное устройство средство для проверки подписанной квитанции получателя платежа.

В частности, упомянутое средство для формирования платежного поручения плательщика, подписанного секретным ключом платежного сертификата, может иметь средство для формирования запроса на кредитование платежного счета, которое, в свою очередь, может иметь средство для понижения уровня подписи платежного сертификата. Назначение средства для понижения уровня подписи платежного сертификата состоит в том, чтобы по имеющейся в платежном устройстве подписи платежного сертификата некоторого уровня изготовить другую подпись платежного сертификата более низкого уровня, предназначенную для доставки в платежный сервер как часть запроса на кредитование платежного счета.

В частности, платежное устройство также может содержать средство для открытия

счета с открытым ключом.

Кроме того, платежное устройство, приемное устройство и платежный сервер могут быть снабжены средствами для шифрования исходящих сообщений и средствами для дешифрования входящих сообщений.

5

Краткое описание фигур чертежей

В дальнейшем предлагаемое изобретение поясняется описанием конкретных примеров его выполнения и прилагаемыми чертежами, на которых:

Фиг.1 изображает блок-схему устройства для проведения платежей;

Фиг.2 изображает блок-схему операции пополнения платежного устройства;

10

Фиг.3 изображает блок-схему платежной операции.

Лучший вариант осуществления изобретения

В лучшем варианте осуществления способа проведения платежей по каждому варианту платежа проводят в рамках платежной системы, оператор которой включает множество банков, и в которой имеется много плательщиков и получателей. Причем как плательщики, так и получатели пользуются устройствами, содержащими одновременно и платежное, и приемное устройство. Далее, при описании лучшего варианта осуществления изобретения, такое устройство называется "Электронным кошельком".

До начала обслуживания клиентов входящий в платежную систему банк проводит подготовительные действия. Поскольку подготовительные действия осуществляют одинаково в лучшем варианте осуществления каждого из вариантов заявленного способа, то ниже приведено отдельное описание лучшего варианта осуществления этих действий.

На этапе подготовительных действий фиксируют систему цифровой подписи, допускающей изготовление цифровой подписи вслепую. Эта система предназначена для изготовления и проверки денежной подписи и называется ниже системой денежной подписи. Также фиксируют набор допустимых уровней, то есть величин, каждая из которых определяет некоторую денежную ценность. При этом набор допустимых уровней выбирается так, чтобы произвольная денежная ценность, представляющая практический интерес при пополнении платежного устройства, была представлена некоторым уровнем. Для каждого допустимого уровня банк выбирает соответствующий ему денежный секретный ключ и соответствующий денежному секретному ключу денежный открытый ключ в рамках фиксированной системы денежной подписи. При этом соответствующие каждому допустимому уровню денежный секретный ключ выбирают так, что подпись уровня A для некоторых данных X , в качестве которых взята подпись уровня B для некоторых данных Y , соответствует подписи уровня $(A + B)$ для данных Y . Информация о денежных открытых ключах и денежных ценностях, соответствующих допустимым уровням публикуется и вносится в запоминающие устройства "Электронных кошельков".

Также фиксируют систему цифровой подписи, предназначенную для подписи сообщений, используемых при проведении платежей. В рамках этой системы банк выбирает секретные ключи и соответствующие открытые ключи. Информация об открытых ключах публикуется и вносится в запоминающие устройства "Электронных кошельков".

Кроме того, фиксируют структуру и критерий действительности основ платежных сертификатов, а также способ включения в основу идентификатора открытого ключа платежного сертификата. Для этого фиксирует одностороннюю хэш-функцию F , которая принимающую значения в битовых последовательностях и, предпочтительно, обладает свойством "collision free". В качестве основ платежных сертификатов принимают пары (Y, X) , где Y открытый ключ подписи платежного сертификата, выбираемый в рамках фиксированной системы подписи и используемый в качестве своего собственного идентификатора. При этом основу с такой структурой считают действительной, если $F(Y)=X$. В качестве идентификатора основы платежного сертификата *BaseId* принимают данные X .

Возможность реализации вышеописанных подготовительных действий лучшего варианта осуществления способа проведения платежей по каждому из заявленных вариантов поясняется следующим примером.

Пример 1

В качестве системы денежной подписи используют систему, основанную на цифровой RSA-подписи (B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, John Wiley&Sons, New York, 2nd edition, 1996 и A. J. Menezes, P. C. Van Oorshot, S. A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1997). В этой системе секретный ключ представляет собой пару (N, D) , где D секретная экспонента, а N модуль. При этом соответствующий открытый ключ представляет собой пару (N, E) , где E открытая экспонента, удовлетворяющая условию $X^{E \cdot D} \equiv 1 \pmod{N}$ для всякого взаимно простого с N целого числа X . Система RSA допускает несколько способов изготовления цифровой подписи вслепую. Например, один из таких способов описан в патенте: D. Chaum, Blind Signature Systems, U.S. Patent 4,759,063, 19 Jul 1988, а другой в патенте: D. Chaum, Blind Unanticipated Signature Systems, U.S. Patent 4,759,064, 19 Jul 1988.

В качестве допустимого уровня принимают произвольный набор неотрицательных целых чисел $L = (L_1, L_2, L_3)$, а выраженная в центах денежная ценность определяется таким уровнем по формуле $L_1 \cdot N_1 + L_2 \cdot N_2 + L_3 \cdot N_3$, где $N_1 = 1$, $N_2 = 100$, $N_3 = 100^2$.

Выбор для каждого допустимого уровня соответствующего ему денежного секретного ключа и соответствующего денежному секретному ключу денежного открытого ключа в рамках системы RSA-подписи осуществляют следующим образом. В качестве модуля каждого из открытых и секретных денежных ключей используют произвольный RSA-модуль N , для которого целые числа $E_1 = 3$, $E_2 = 17$, $E_3 = 5$ допустимы в качестве открытых экспонент. Ниже числа E_1 , E_2 , E_3 называются базовыми открытыми экспонентами. В качестве открытого денежного ключа, соответствующего уровню L , принимают ключ с открытой экспонентой $E = E_1^{L_1} \cdot E_2^{L_2} \cdot E_3^{L_3}$. В качестве секретного денежного ключа, соответствующего уровню L , принимают ключ с секретной экспонентой $D = D_1^{L_1} \cdot D_2^{L_2} \cdot D_3^{L_3}$, где D_j секретная экспонента, соответствующая базовой открытой экспоненте E_j . Средства для создания ключей в системе RSA хорошо известны (B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, John Wiley&Sons, New York, 2nd edition, 1996 и A. J. Menezes, P. C. Van Oorshot, S. A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1997). В качестве информации о денежных открытых ключах публикуются модуль N и базовые открытые экспоненты

E_1, E_2, E_3 . В качестве информации о денежных ценностях, соответствующих допустимым уровням публикуются данные $N_1 = 1, N_2 = 100, N_3 = 100^2$.

В качестве односторонней хэш-функции F , используемой в критерии действительности основ платежных сертификатов, фиксируют функцию, которая на последовательности битов X принимает значение, полученное конкатенацией битовых последовательностей $H(X)$ и Y , где H обозначает известную хэш-функцию SHA-1 (A. J. Menezes, P. C. Van Oorshot, S. A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1997, p. 348), а $Y = 1111...1110$, причем число единичных битов в Y таково, что общее число битов $F(X)$ равно числу битов в модуле N .

В качестве системы цифровой подписи, предназначенной для подписи сообщений, используемых при проведении платежей, фиксируют систему RSA с открытой экспонентой 3, то есть систему RSA, в которой открытая экспонента фиксирована и равна 3. В рамках этой системы банк выбирает секретный ключ DB и соответствующий открытый ключ EB . В качестве информации об открытом ключе EB публикуется его модуль.

Ниже приведено описание лучшего варианта осуществления способа проведения платежей по первому варианту.

После проведения вышеописанных подготовительных действий получатель платежа открывает в банке счет с открытым ключом. При этом открытие счета осуществляется следующим образом.

В качестве секретного ключа открываемого счета получатель платежа принимает свой секретный ключ, созданный непосредственно для этой цели в рамках системы подписи, фиксированной на этапе подготовительных действий. Открытый ключ, соответствующий секретному ключу счета доставляют по открытым телекоммуникационным сетям в платежный сервер. В платежном сервере доставленный открытый ключ принимают в качестве открытого ключа открываемого счета, присваивают открываемому счету номер и создают в хранилище счетов запись, содержащую номер счета, открытый ключ счета и иные атрибуты счета. Получатель платежа считает счет открытым после получения подписанного секретным ключом банка сообщения, которое подтверждает открытие счета, связанного с открытым ключом счета. При этом подпись этого сообщения сохраняют в запоминающем устройстве "Электронного кошелька", что позволит в последующем предъявить банку обоснованные претензии в случае невыполнения им своих обязательств по открытому счету.

Преимущества описанного варианта открытия счета состоят в том, что операция открытия счета происходит удаленным образом в режиме реального времени. Кроме того, открытие в платежном сервере происходит автоматически, так как, в частности, не требует проверок идентифицирующих личность владельца счета данных. Тем самым такой вариант открытия счета весьма экономичен для банка и очень удобен для клиентов банка. Кроме того, счет, открытый вышеописанным образом, как и всякий счет с открытым ключом допускает безопасное удаленное управление, а относительно короткий номер счета позволяет воспроизводить его вручную, в частности, для указания цели почтового перевода денег.

В качестве источника пополнения своего "Электронного кошелька" в лучшем варианте осуществления плательщик использует произвольное средство для денежных операций, допускающее удаленное и безопасное управление.

При создании основы *Base* платежного сертификата в процессе проведения операции первичного наполнения платежного сертификата в качестве секретного ключа плательщика *DP* и соответствующего ему открытого ключа *EP* выбирают специально созданные для этой цели ключи. При этом ключи *DP* и *EP* выбирают в рамках фиксированной на этапе подготовительных действий системы подписи.

При проведении операции первичного наполнения платежного сертификата замаскированный идентификатор *BaseId* основы платежного сертификата доставляют в платежный сервер как часть денежного запроса. При этом в денежный запрос включают также данные, необходимые для удаленного востребования средств с используемого источника пополнения.

До проведения платежной операции данные обязательства получателя платежа по платежу подписывают произвольным секретным ключом получателя платежа, а перед принятием решения плательщика о проведении платежной операции в платежном устройстве проверяют правильность подписи для данных обязательства получателя платежа по платежу и сохраняют подписанные данные обязательства получателя платежа по платежу.

При проведении платежной операции в платежное поручение плательщика в качестве сведений о получателе платежа включают идентификатор счета получателя платежа и условия платежа. В условия платежа включают результат обработки данных обязательства получателя платежа по платежу фиксированной односторонней функцией. Платежное поручение плательщика шифруют шифровальным ключом оператора.

В платежное поручение получателя платежа включают сессионный ключ для симметричного шифрования, а само платежное поручение получателя платежа шифруют шифровальным ключом оператора.

В ответ оператора на платежное поручение получателя платежа включают квитанцию получателя платежа, подписанную секретным ключом оператора, а ответ оператора на платежное поручение получателя платежа шифруют содержащимся в платежном поручении получателя платежа сессионным ключом. Получатель платежа судит о проведении платежа по правильности подписи для квитанции получателя платежа.

В приемном устройстве по ответу оператора на платежное поручение получателя платежа формируют и доставляют в платежное устройство данные, подтверждающие согласие получателя платежа с фактом завершенности платежной операции.

Неизрасходованную на цели платежа часть стоимости платежного сертификата, возвращают в платежное устройство в качестве сдачи.

Возможность реализации вышеописанного лучшего варианта осуществления способа проведения платежей по первому варианту поясняется следующим примером.

Пример 2

Подготовительные действия осуществляют как в вышеописанном примере 1. Получатель платежа, являющийся в данном примере продавцом, открывает в банке счет с открытым ключом *ES* как это описано выше. При этом в запоминающем устройстве "Электронного кошелька" продавца создается запись с информацией об открытом счете, содержащая секретный ключ *DS*, соответствующий открытому ключу *ES*, номер *AccountId* открытого счета и иные атрибуты счета.

В качестве источника пополнения своего "Электронного кошелька" в этом примере плательщик использует свой счет, который он открывает точно так, как и получатель платежа. На открытый им счет плательщик доставляет почтовым переводом некоторую сумму денег, для определенности 100 долларов.

- 5 Плательщик пополняет свой "Электронный кошелек" посредством операции первичного наполнения платежного сертификата, используя в качестве источника пополнения открытый счет.

- 10 При проведении операции первичного наполнения платежного сертификата создание основы платежного сертификата осуществляют выбором секретного ключа подписи DP и соответствующего ему открытого ключа подписи EP и в рамках системы RSA с открытой экспонентой 3. Поскольку открытая экспонента фиксирована, то открытый ключ представлен одним модулем. Как указано выше, средства для создания таких ключей хорошо известны. В качестве основы платежного сертификата (Y, X) берут данные (EP, X) , где X получают по ключу EP средством для вычисления функции F , описанной в вышеприведенном примере 1. Такое средство реализуют программным образом на основе вышеприведенного описания для функции F .

- 15 При проведении операции первичного наполнения платежного сертификата замаскированный идентификатор $BaseId$ основы платежного сертификата доставляют в платежный сервер как часть денежного запроса. В денежный запрос включают также требуемую сумму пополнения, для определенности 200 долларов, и номер счета плательщика, а вместе с денежным запросом в платежный сервер доставляют его подпись секретным ключом счета плательщика. При этом пополнение платежного устройства осуществляют из средств указанного в денежном запросе счета, предварительно проверив содержащуюся в денежном запросе подпись открытым ключом
- 20 указанного в денежном запросе счета.

- 25 Для маскировки идентификатора $BaseId$ основы платежного сертификата выбирают такой уровень $M = (M_1, M_2, M_3)$, что L_1 не превышает M_1 , L_2 не превышает M_2 , а L_3 не превышает M_3 , где $L = (L_1, L_2, L_3)$ уровень того денежного секретного ключа, который будет использован в платежном сервере при пополнении платежного устройства. Такой выбор уровня M осуществляют по требуемой сумме пополнения, выраженной в центах, то есть в этом примере равной 20 000. При выборе уровня M имеют в виду, что уровень L используемого банком денежного секретного ключа определяют по заранее фиксированному в платежной системе правилу следующим образом.

- 30 Для маскировки идентификатора $BaseId$ основы платежного сертификата выбирают такой уровень $M = (M_1, M_2, M_3)$, что L_1 не превышает M_1 , L_2 не превышает M_2 , а L_3 не превышает M_3 , где $L = (L_1, L_2, L_3)$ уровень того денежного секретного ключа, который будет использован в платежном сервере при пополнении платежного устройства. Такой выбор уровня M осуществляют по требуемой сумме пополнения, выраженной в центах, то есть в этом примере равной 20 000. При выборе уровня M имеют в виду, что уровень L используемого банком денежного секретного ключа определяют по заранее фиксированному в платежной системе правилу следующим образом.
- 35 Сначала по содержащейся в денежном запросе требуемой сумме и по средствам, находящимся на счете плательщика, определяют сумму пополнения. В этом примере, к моменту проведения операции пополнения средства счета, выраженные в центах, составляют величину 19 975. Эта сумма сложилась следующим образом. При зачислении на счет 20 000 центов, что соответствует 200 долларам почтового перевода, банк взял комиссию в размере 50 центов и на счете оказалось 19 950 центов. За время прошедшее с момента зачисления на счет этой суммы до момента начала операции пополнения платежного устройства банк, во-первых, начислил проценты в размере 30 центов, а, во-вторых, взял плату за текущее обслуживание счета в размере 5 центов. В итоге, к моменту проведения операции пополнения средства счета со-
- 40

ставляют величину 19 975 центов. Кроме того, за операцию пополнения платежного устройства банк берет плату в размере 60 центов. Таким образом, сумма пополнения составляет в этом примере 19 915 центов. Уровень L определяют по сумме пополнения, в этом примере равной 19 915, с помощью фиксированного в платежной системе правила так, чтобы выполнялось соотношение $L_1 \cdot N_1 + L_2 \cdot N_2 + L_3 \cdot N_3 = 19\,915$ центов. В данном примере $L = (1, 99, 15)$.

В любом случае, фиксированное правило определения уровня L по требуемой сумме пополнения, гарантирует, в этом примере, что L_1 не превосходит 2, а L_2 и L_3 не превосходят 99. Таким образом, в качестве уровня M берут данные $(2, 99, 99)$.

После выбора уровня M маскировку исходных данных X , в качестве которых при первичном наполнении платежного сертификата используют идентификатор *BaseId* основы платежного сертификата, производят в соответствии с соотношением $X' = F \cdot X \pmod{N}$, где $F = R^U \pmod{N}$, $U = U_1 \cdot U_2 \cdot U_3$, $U_1 = E_1^{M_1}$, $U_2 = E_2^{M_2}$, $U_3 = E_3^{M_3}$, а R рандомизированное целое число подходящего размера.

В платежном сервере в качестве данных для демаскировки S' изготавливают подпись замаскированных данных X' денежным секретным ключом, соответствующим уровню L . Тем самым, в этом примере данные X' обрабатывают денежным секретным ключом с модулем N и секретной экспонентой $D = D_1^{L_1} \cdot D_2^{L_2} \cdot D_3^{L_3}$. После этого данные S' доставляют в платежное устройство.

В "Электронном кошельке" плательщика по полученным данным для демаскировки S' изготавливают подпись платежного сертификата S демаскировкой полученных данных S' , которую осуществляют в соответствии с соотношением $S = S' \cdot T^{-1} \pmod{N}$, где $T = R^V \pmod{N}$, $V = V_1 \cdot V_2 \cdot V_3$, а $V_1 = E_1^{M_1-L_1}$, $V_2 = E_2^{M_2-L_2}$, $V_3 = E_3^{M_3-L_3}$. Изготовленную подпись S сохраняют в запоминающем устройстве. В итоге в "Электронном кошельке" плательщика оказывается платежный сертификат стоимостью 19 915 центов.

Плательщик, желая заплатить продавцу 43.50 доллара за некоторый товар, готовит платежные данные *PaymentData* включая в них платежное поручение плательщика *PayerOrder*, подписанное секретным ключом платежного сертификата DP , и данные A , предназначены для продавца и состоящие в данном примере из наименования оплачиваемого товара и идентификационных данных получателя товара. Платежное поручение плательщика *PayerOrder* состоит из открытого ключа платежного сертификата EP , подписи платежного сертификата S , номера счета продавца *AccountId* и данных C , определяющих условия платежа. В данном примере в качестве C плательщик берет номер счета продавца *AccountId* и хэш-функции H от текста обязательства, которое принимает на себя продавец в случае проведения платежа, а именно обязательства предоставить соответствующий товар лицу с указанными идентификационными данными.

Продавец, желая принять платеж, формирует свое платежное поручение *SellerOrder* = (*AccountId*, *PayerOrder*), зашифрованное открытым шифровальным ключом банка, и доставляет его в банк.

Банк, убедившись, что в списке использованных платежных сертификатов отсутствует запись о платежном сертификате с открытым ключом EP , проверив подпись платежного поручения плательщика *PayerOrder* открытым ключом платежного сертификата EP , и, проверив правильность подписи S платежного сертификата, заносит в спи-

сок использованных платежных сертификатов запись, включающую открытый ключ *EP* и подписанное платежное поручение плательщика *PayerOrder*, кредитует счет с номером *AccountId* на сумму 43.49 долларов, в предположении, что стоимость проведения платежной операции банком равна 1 центу. После этого банк формирует квитанцию продавца, подтверждающую факт кредитования счета с номером *AccountId* на сумму 43.49 долларов, подписывает ее и доставляет продавцу, который, проверив правильность подписи банка для полученной квитанции, считает платеж проведенным и сообщает плательщику об успешном проведении платежа.

Возврат остатка платежного сертификата, в этом примере составляющем величину (19 915 - 4 350) центов, осуществляют пополнением платежного устройства, причем такое пополнение может быть осуществлено как посредством первичного наполнения платежного сертификата, так и пополнением уже имеющегося платежного сертификата. Для этого в платежное поручение плательщика включают замаскированную подпись того платежного сертификата, стоимость которого возрастет за счет возвращаемого остатка, в ответ оператора на платежное поручение получателя включают соответствующую денежную подпись оператора, доставляемую в платежное устройство через приемное устройство вместе с другими данными.

Ниже приведено описание лучшего варианта осуществления способа проведения платежей по второму варианту.

В лучшем варианте осуществления способа проведения платежей по второму варианту осуществляют все действия, которые проводят в лучшем варианте осуществления способа проведения платежей по первому варианту.

Кроме того, дополнительно проводят операцию пополнения платежного сертификата, которая реализована так, что операция первичного наполнения платежного сертификата неотличима для оператора от операции пополнения платежного сертификата. Операцию пополнения платежного сертификата проводят в произвольный момент времени перед платежной операцией и используют для пополнения платежного сертификата, стоимость которого недостаточна для проведения платежной операции.

Возможность реализации вышеописанного лучшего варианта осуществления способа проведения платежей по четвертому варианту пояснена вышеописанным примером 2, в котором пояснена возможность реализации лучшего варианта осуществления способа проведения платежей по первому варианту, и следующим примером 3, в котором пояснена возможность реализации лучшего варианта осуществления пополнения платежного устройства посредством пополнения платежного сертификата.

35 Пример 3

В этом примере используются соглашения и обозначения, принятые в вышеописанном примере 1.

Операцию пополнения платежного сертификата, то есть операцию получения подписи платежного сертификата, уровень которой превышает уровень той подписи платежного сертификата, которая имеется в платежном устройстве к началу операции пополнения, осуществляют посредством изготовления вслепую денежной подписи оператора. При этом в качестве исходных данных берут имеющуюся в платежном устройстве подпись платежного сертификата.

Предположим, что в "Электронном кошельке" плательщика имеется платежный

- сертификат с подписью S_1 уровня $(0, 2, 30)$. Предположим, что для совершения некоторой покупки плательщику не достаточно стоимости этого платежного сертификата, которая в данном случае равна двум долларам и тридцати центам. Для того, чтобы все же осуществить такую покупку, плательщик пополняет свой "Электронный кошелек" 5 пополнением платежного сертификата.

- Для этого замаскированную подпись S_1 платежного сертификата доставляют в платежный сервер как часть денежного запроса. В денежный запрос включают также требуемую сумму пополнения, для определенности 50 долларов, номер счета плательщика, а вместе с денежным запросом в платежный сервер доставляют его подпись 10 секретным ключом счета плательщика. При этом пополнение платежного устройства осуществляют из средств указанного в денежном запросе счета, предварительно проверив содержащуюся в денежном запросе подпись открытым ключом указанного в денежном запросе счета.

- Для маскировки подписи S_1 платежного сертификата, как и в вышеприведенном 15 примере 2, выбирают такой уровень $M = (M_1, M_2, M_3)$, что L_1 не превышает M_1 , L_2 не превышает M_2 , а L_3 не превышает M_3 , где $L = (L_1, L_2, L_3)$ уровень того денежного секретного ключа, который будет использован в платежном сервере при пополнении платежного устройства. Выбор уровня M осуществляют по требуемой сумме пополнения, как и в примере 2. В данном примере $M = (0, 5, 99)$.

- 20 Как и в примере 2, по содержащейся в денежном запросе требуемой сумме и по средствам, находящимся на счете плательщика, определяют сумму пополнения. Предположим, что сумма пополнения в этом примере оказалась равной 47 долларам и 13 центам, то есть 4 713 центам. Уровень L определяют по сумме пополнения, как и в примере 2. В данном примере $L = (0, 47, 13)$.

- 25 После выбора уровня M маскировку исходных данных X , в качестве которых при первичном наполнении платежного сертификата используют идентификатор *BaseId* основы платежного сертификата, производят в соответствии с соотношением $X' = F \cdot X \pmod{N}$, где $F = R^U \pmod{N}$, $U = U_1 \cdot U_2 \cdot U_3$, $U_1 = E_1^{M_1}$, $U_2 = E_2^{M_2}$, $U_3 = E_3^{M_3}$, а R рандомизированное целое число подходящего размера.

- 30 В платежном сервере в качестве данных для демаскировки S' изготавливают подпись замаскированных данных X' денежным секретным ключом, соответствующим уровню L . Тем самым, в этом примере данные X' обрабатывают денежным секретным ключом с модулем N и секретной экспонентой $D = D_1^{L_1} \cdot D_2^{L_2} \cdot D_3^{L_3}$. После этого данные S' доставляют в платежное устройство.

- 35 В "Электронном кошельке" плательщика по полученным данным для демаскировки S' изготавливают подпись платежного сертификата S демаскировкой полученных данных S' , которую осуществляют в соответствии с соотношением $S = S' \cdot T^{-1} \pmod{N}$, где $T = R^V \pmod{N}$, $V = V_1 \cdot V_2 \cdot V_3$, а $V_1 = E_1^{M_1-L_1}$, $V_2 = E_2^{M_2-L_2}$, $V_3 = E_3^{M_3-L_3}$. Изготовленную 40 подпись S сохраняют в запоминающем устройстве, вместо ранее имевшейся подписи S_1 . При этом уровень подписи S равен сумме уровня подписи S_1 , то есть в данном примере $(0, 2, 30)$, и уровня $L = (0, 47, 13)$. Таким образом, уровень подписи S равен $(0, 49, 43)$, а стоимость платежного сертификата повысилась до 49 долларов и 43 центов.

Ниже приведено описание лучшего варианта осуществления способа проведения

платежей по третьему варианту.

Подготовительные действия, открытие счета получателя платежа, пополнение платежного устройства плательщика и действия получателя платежа при проведении платежной операции осуществляют, как и в вышеописанном лучшем варианте осуществления способа проведения платежей по первому варианту.

Как и в вышеописанном лучшем варианте осуществления способа проведения платежей по первому варианту перед принятием решения плательщика о проведении платежной операции в платежном устройстве проверяют правильность подписи для данных обязательства получателя платежа по платежу и сохраняют подписанные данные обязательства получателя платежа по платежу.

При проведении платежной операции в платежное поручение плательщика в качестве сведений о получателе платежа включают идентификатор счета получателя платежа и условия платежа. В условия платежа включают результат обработки данных обязательства получателя платежа по платежу фиксированной односторонней функцией. Платежное поручение плательщика шифруют шифровальным ключом оператора.

В платежное поручение получателя платежа включают сессионный ключ для симметричного шифрования, а само платежное поручение получателя платежа шифруют шифровальным ключом оператора.

В ответ оператора на платежное поручение получателя платежа включают квитанцию получателя платежа, подписанную секретным ключом оператора, а ответ оператора на платежное поручение получателя платежа шифруют содержащимся в платежном поручении получателя платежа сессионным ключом. Получатель платежа судит о проведении платежа по правильности подписи для квитанции получателя платежа.

В приемном устройстве по ответу оператора на платежное поручение получателя платежа формируют и доставляют в платежное устройство данные, подтверждающие согласие получателя платежа с фактом завершения платежной операции.

Оператор открывает связанный с каждым платежным сертификатом платежный счет и связывает его с открытым ключом подписи платежного сертификата, причем средства платежного счета расходуются при одной или нескольких платежных операциях. При этом в качестве платежного счета используют счет с открытым ключом, совпадающим с открытым ключом платежного сертификата. Средства на платежном счете оказываются в результате одной или нескольких операций кредитования платежного счета, производимого из средств заключенной в платежном сертификате стоимости, а операцию открытия платежного счета совмещают с первой по времени операцией его кредитования.

При операции кредитования платежного счета в платежный сервер доставляют подпись платежного сертификата, уровень которой выбирают произвольно в пределах уровня платежного сертификата. Более того, каждую операцию кредитования платежного счета совмещают с одной из платежных операций.

Возможность реализации вышеописанного лучшего варианта осуществления способа проведения платежей по третьему варианту поясняется следующим примером.

Пример 4

В этом примере используются обозначения и соглашения, принятые в примере 1.

Подготовительные действия, открытие счета продавца, пополнение платежного устройства плательщика и действия продавца при проведении платежной операции осуществляют в этом примере, как и в вышеописанном примере 2.

Ниже приведены примеры трех платежных операций. При этом первую из описанных ниже платежных операций, которая является первой по времени операцией, проводимую с использованием платежного сертификата, совмещают с операцией открытия платежного счета и его кредитования. Вторую из описанных ниже платежных операций совмещают с операцией кредитования уже открытого платежного счета. Третью из описанных ниже платежных операций проводят в условиях, когда на платежном счете уже имеется достаточно средств для проведения такой платежной операции.

Ниже приведено описание первой по времени платежной операции, проводимой с использованием платежного сертификата, которую совмещают с операцией открытия платежного счета и его кредитования.

Предположим, что в платежном устройстве имеется платежный сертификат с основой (EP, X) и подписью S уровня $(2, 12, 45)$. Стоимость этого платежного сертификата равна 212 долларам и 45 центам. Предположим, кроме того, что этот платежный сертификат еще не использовался ни при одной платежной операции.

Платательщик, желая заплатить продавцу сумму в 18.999 доллара за некоторый товар, готовит платежные данные *PaymentData*, включая в них платежное поручение плательщика *PayerOrder*, подписанное секретным ключом платежного сертификата DP , и данные A , предназначены для продавца и состоящие в данном примере из наименования оплачиваемого товара и идентификационных данных получателя товара.

Платежное поручение плательщика *PayerOrder* состоит из открытого ключа платежного сертификата EP , подписи платежного сертификата S_I , номера счета продавца *AccountId* и данных C , определяющих условия платежа. В данном примере в качестве C плательщик берет номер счета продавца *AccountId* и хэш-функции H от текста обязательства, которое принимает на себя продавец в случае проведения платежа, а именно обязательства предоставить соответствующий товар лицу с указанными идентификационными данными.

Включаемый в платежное поручение плательщика *PayerOrder* открытый ключ EP используется в платежном сервере для открытия платежного счета, связанного с этим ключом. Включаемую в платежное поручение плательщика *PayerOrder* подпись платежного сертификата S_I используется в платежном сервере для кредитования платежного счета с открытым ключом EP .

Подпись S_I изготавливают в платежном устройстве по подписи платежного сертификата S . При этом уровень $L=(L_1, \dots, L_3)$ подписи S_I выбирают так, чтобы, с одной стороны, соответствующей этому уровню стоимости было достаточно для проведения данной платежной операции, а, с другой стороны, чтобы в каждом из трех разрядов он был не больше уровня подписи S . Еще одна цель такого выбора состоит в том, чтобы не раскрыть оператору платежной системы уровень имеющейся в платежном устройстве подписи S . В данном примере уровень подписи S представлен набором $(2, 12, 45)$, а выраженная в центах стоимость, достаточная для проведения данной платежной операции, составляет, в данном случае, 1899.9 центов. Тем самым на выбор уровня

$L=(L_1, \dots, L_3)$ имеются следующие ограничения: во-первых, L_1 не превосходит 2, L_2 не превосходит 12, L_3 не превосходит 45, а, во-вторых, величина $L_1 \cdot N_1 + L_2 \cdot N_2 + L_3 \cdot N_3$, где $N_1 = 1$, $N_2 = 100$, $N_3 = 100^2$, должна быть не меньше, чем 1899.9 центов. Уровень L , удовлетворяющий этим условиям, выбирают с помощью датчика случайных чисел и, в данном примере, $L=(1, 3, 14)$. Подпись S_l изготавливают вычислительным устройством, запрограммированным соответствующим образом, в соответствии с соотношением $S_l = S^V \pmod{N}$, где $V = V_1 \cdot V_2 \cdot V_3$, $V_1 = E_1^{M_1-L_1}$, $V_2 = E_2^{M_2-L_2}$, $V_3 = E_3^{M_3-L_3}$, а уровень (M_1, \dots, M_3) равен уровню $(2, 12, 45)$, то есть уровню подписи S .

Продавец, желая принять платеж, формирует свое платежное поручение $SellerOrder = (AccountId, PayerOrder)$, зашифрованное открытым шифровальным ключом банка, и доставляет его в банк.

Банк, убедившись, что в базе данных платежных счетов отсутствует запись о платежном счете с открытым ключом EP , и, проверив правильность подписи S_l открытым или секретным денежным ключом, открывает платежный счет, внося в базу данных платежных счетов соответствующую запись. При этом, во-первых, открытый счет кредитруется на сумму, соответствующую уровню $L=(1, 3, 14)$ подписи S_l , то есть в данном примере, на сумму в 103 доллара и 14 центов. Кроме того, в расходы открытого платежного счета записывается сумма 50 центов, равная плате за открытие платежного счета. После этого проводится собственно платежная операция. А именно, проверив подпись платежного поручения плательщика $PayerOrder$ открытым ключом платежного счета EP , банк заносит в информационное хранилище подписанное платежное поручение плательщика $PayerOrder$, увеличивает величину расходов платежного счета на сумму 1899.9 и кредитует счет с номером $AccountId$ на сумму 1799.9 центов, в предположении, что стоимость проведения платежной операции банком равна 1 центу. После этого банк формирует квитанцию продавца, подтверждающую факт кредитования счета с номером $AccountId$ на сумму 1799.9 центов, подписывает ее и доставляет продавцу, который, проверив правильность подписи банка для полученной квитанции, считает платеж проведенным и сообщает плательщику об успешном проведении платежа.

Ниже приведено описание платежной операции, которую совмещают с операцией кредитования уже открытого платежного счета. Получатель платежа, участвующий в этой операции, вообще говоря, никак не связан с получателем платежа из вышеописанной первой платежной операции.

Предположим, что в платежном устройстве имеется платежный сертификат с основой (EP, X) и подписью S уровня $(2, 12, 45)$. Стоимость этого платежного сертификата равна 212 долларам и 45 центам. Предположим, что платежный счет, связанный с данным сертификатом уже открыт, суммарная величина расходов этого платежного счета не превышает величины в 6732.8 цента, а уровень подписи доставленной оператору при одной из предыдущих операций кредитования платежного счета не превышает уровня $(1, 3, 14)$. Тем самым, платежный счет при предыдущих операциях кредитования прокредитован на сумму в 10 314 центов.

Плательщик, желая заплатить продавцу сумму в 3699.9 центов за некоторый товар, готовит платежные данные $PaymentData$, включая в них платежное поручение плательщика $PayerOrder$, подписанное секретным ключом платежного сертификата DP , и

данные A , предназначены для продавца и состоящие в данном примере из наименования оплачиваемого товара и идентификационных данных получателя товара.

Так как сумма платежа превосходит разность между суммой в 10 314 центов, доставленной на платежный счет при предыдущих операциях кредитования, и суммарной величиной расходов этого платежного счета, составляющей 6732.8 цента, то 5 плательщик совмещает платежную операцию с операцией кредитования платежного счета.

Платежное поручение плательщика *PayerOrder* состоит из идентификатора открытого ключа платежного сертификата, в качестве которого в этом примере используется значение заранее фиксированной хэш-функции H на ключе EP , подписи платежного сертификата S_I , номера счета продавца *AccountId* и данных C , определяющих условия платежа. В данном примере в качестве C плательщик берет номер счета продавца *AccountId* и хэш-функции H от текста обязательства, которое принимает на себя продавец в случае проведения платежа, а именно обязательства предоставить соответствующий товар лицу с указанными идентификационными данными.

Включаемый в платежное поручение плательщика *PayerOrder* идентификатор открытого ключа платежного сертификата $H(EP)$ используется в платежном сервере для поиска платежного счета, связанного с ключом EP . Включаемую в платежное поручение плательщика *PayerOrder* подпись платежного сертификата S_i используется в платежном сервере для кредитования платежного счета с открытым ключом EP .

Подпись S_i изготавливают в платежном устройстве по подписи платежного сертификата S . При этом уровень $L = (L_1, \dots, L_3)$ подписи S_i выбирают так, чтобы, во-первых, соответствующей этому уровню стоимости было достаточно для проведения данной платежной операции с учетом ранее проведенных расходов, во-вторых, чтобы в каждом из трех разрядов он был не больше уровня подписи S , и, в третьих, чтобы в каждом из трех разрядов он был не меньше уровня подписи доставленной оператору при одной из предыдущих операций кредитования платежного счета, то есть в этом примере уровни $(1, 3, 14)$. В данном примере берут $L = (2, 7, 15)$. Подпись S_i изготавливают вычислительным устройством, запрограммированным соответствующим образом, в соответствии с соотношением $S_i = S^V \pmod{N}$, где $V = V_1 \cdot V_2 \cdot V_3$, $V_1 = E_1^{M_1-L_1}$, $V_2 = E_2^{M_2-L_2}$, $V_3 = E_3^{M_3-L_3}$, а уровень (M_1, \dots, M_3) равен уровню $(2, 12, 45)$, то есть уровню подписи S .

Продавец, желая принять платеж, формирует свое платежное поручение *SellerOrder* = (*AccountId*, *PayerOrder*), зашифрованное открытым шифровальным ключом банка, и
35 доставляет его в банк.

Банк, обнаружив в базе данных платежных счетов запись о платежном счете с открытым ключом EP , и, проверив правильность подписи S_1 открытым или секретным денежным ключом, увеличивает общую сумму средств найденного счета до величины, соответствующую такому уровню, каждый разряд которого равен максимуму из соответствующих разрядов уровней всех подписей платежного сертификата, доставленных в банк при операциях кредитования данного платежного счета. После этого проводится собственно платежная операция. Эта операция проводится так же, как и в вышеприведенном примере первой платежной операции.

Ниже приведено описание платежной операции, которую проводят с помощью уже

открытого платежного счета без совмещения с операцией кредитования платежного счета. Получатель платежа, участвующий в этой операции, вообще говоря, никак не связан с получателем платежа из вышеописанной первой платежной операции.

5 Таковую операцию проводят в том случае, когда сумма платежа не превосходит разности между суммой, доставленной на платежный счет при предыдущих операциях кредитования, и суммарной величиной расходов этого платежного счета. При такой операции платежное поручение плательщика *PayerOrder* не содержит подписи платежного сертификата, а состоит из идентификатора открытого ключа платежного сертификата, в качестве которого в этом примере используется значение заранее фиксированной хэш-функции *H* на ключе *EP*, номера счета продавца *AccountId* и данных *C*, 10 определяющих условия платежа. В данном примере в качестве *C* плательщик берет номер счета продавца *AccountId* и хэш-функции *H* от текста обязательства, которое принимает на себя продавец в случае проведения платежа, а именно обязательства предоставить соответствующий товар лицу с указанными идентификационными данными. В остальном, такая операция проходит так же, как и вышеописанные платежные операции. 15

Ниже приведено описание лучшего варианта осуществления способа проведения платежей по четвертому варианту.

20 В лучшем варианте осуществления способа проведения платежей по четвертому варианту осуществляют все действия, которые проводят в лучшем варианте осуществления способа проведения платежей по третьему варианту. Кроме того, дополнительно проводят операцию пополнения платежного сертификата, причем лучший вариант осуществления этой операции описан выше при описании лучшего варианта осуществления способа проведения платежей по второму варианту.

25 Возможность реализации вышеописанного лучшего варианта осуществления способа проведения платежей по четвертому варианту пояснена вышеописанным примером 4, в котором пояснена возможность реализации лучшего варианта осуществления способа проведения платежей по третьему варианту, и вышеописанным примером 3, в котором пояснена возможность реализации лучшего варианта осуществления пополнения платежного устройства посредством пополнения платежного сертификата. 30

Ниже приведено описание лучшего варианта выполнения устройства для проведения платежей.

35 В лучшем варианте платежное устройство содержит средство для пополнения платежного устройства с использованием изготовления вслепую денежной подписи оператора, которое реализовано средством для повышения уровня подписи платежного сертификата. Кроме того, платежное устройство содержит средство для открытия счета с открытым ключом. Помимо этого, средство для формирования платежного поручения плательщика, подписанного секретным ключом платежного сертификата, имеет средство для формирования запроса на кредитование платежного счета, которое, в 40 свою очередь, имеет средство для понижения уровня подписи платежного сертификата.

Приемное устройство содержит средство для открытия счета с открытым ключом и средство для проверки подписанной квитанции получателя платежа открытым ключом оператора.

Платежный сервер содержит средство для обслуживания базы данных платежных счетов и средство для обслуживания базы данных счетов, причем средство для обслуживания базы данных счетов имеет средство для открытия счета с открытым ключом, средство для кредитования счета и средство для списывания со счета средств. Средство для обслуживания базы данных платежных счетов имеет средство для открытия платежного счета, средство для проверки денежной подписи и средство для кредитования платежного счета. Имеющееся в платежном сервере средство для проведения платежной операции имеет средство для проверки подписи платежного поручения плательщика и средство для изготовления подписанной квитанции получателя платежа. Кроме того, платежный сервер содержит средство для изготовления подписанной квитанции получателя платежа.

Средства для сохранения информации в запоминающем устройстве платежного устройства, приемного устройства и платежного сервера имеют высокую надежность, а платежное устройство, приемное устройство и платежный сервер снабжены средствами для шифрования исходящих сообщений и средствами для дешифрования входящих сообщений.

Возможность реализации вышеописанного лучшего варианта выполнения устройства для проведения платежей и использование такого устройства поясняется следующим примером.

20 Пример 5

Пример проиллюстрирован Фиг.1, Фиг.2 и Фиг.3. На Фиг.1 изображена блок-схема устройства для проведения платежей, содержащего платежный сервер 1, платежное устройство 2 и приемное устройство 3. При этом линиями, проведенными между блоками, показаны соединения между вышеуказанными устройствами посредством телекоммуникационных сетей.

На Фиг.2 изображена блок-схема операции пополнения платежного устройства. При этом блок 4 изображает средство для создания основы платежного сертификата обработкой односторонней функцией открытого ключа платежного сертификата, блок 5 изображает запоминающее устройство, линия 6 изображает средство для сохранения созданной основы платежного сертификата в запоминающем устройстве, блок 7 изображает средство для повышения уровня подписи платежного сертификата, блок 8 изображает средство формирования денежного запроса, включающего замаскированную подпись платежного сертификата, блок 9 изображает средство для демаскировки содержащихся в ответе на денежный запрос данных для демаскировки, линия 10 изображает средство для занесения результата демаскировки в запоминающее устройство, блок 11 изображает средство для обработки денежного запроса, а блок 12 изображает средство для изготовления денежной подписи. Кроме того, линия 13 изображает средство для считывания из запоминающего устройства подписи платежного сертификата, линия 14 изображает соединение, по которому денежный запрос доставляют в платежный сервер, а линия 15 изображает соединение, по которому в платежное устройство доставляют ответ оператора на денежный запрос.

На Фиг.3 изображена блок-схема платежной операции. При этом блок 16 изображает средство для формирования платежного поручения плательщика, подписанного секретным ключом платежного сертификата, блок 17 изображает средство для форми-

рования платежного поручения получателя платежа, включающего платежное поручение плательщика, блок 18 изображает средство для проверки подписанной квитанции получателя платежа, блок 19 изображает средство для проведения платежной операции, блок 20 изображает базу данных платежных счетов, блок 21 изображает базу данных счетов. Кроме того, линия 22 изображает соединение, по которому платежное поручение плательщика доставляют в приемное устройство, линия 23 изображает соединение, по которому в платежный сервер доставляют платежное поручение получателя платежа, линия 24 изображает взаимодействие средства для проведения платежной операции с базой данных платежных счетов, линия 25 изображает взаимодействие средства для проведения платежной операции с базой данных счетов, а линия 26 изображает соединение, по которому в приемное устройство доставляют ответ оператора на платежное поручение получателя платежа.

Устройство для проведения платежа реализуется программным образом на основе алгоритмов, указанных в вышеприведенных примерах 2 и 3. В частности, используемые криптографические средства, такие как изготовление подписи, проверка подписи, шифрование и дешифрование, основаны на функциях арифметики целых чисел и модулярной арифметики. Примеры реализации таких функций хорошо известны. Средства для вычисления используемых хэш-функций также хорошо известны.

С помощью платежного устройства, изображенного на Фиг.1, платежи проводят следующим образом.

Платежное устройство 2 пополняют произвольное число раз. При этом, возможно использовать как пополнение платежного устройства первичным наполнением платежного сертификата, так и пополнением одного из уже имеющихся платежных сертификатов. При пополнении платежного устройства первичным наполнением платежного сертификата используется средство для создания основы платежного сертификата, в котором происходит обработкой односторонней функцией открытого ключа платежного сертификата, после чего созданная основа платежного сертификата по линии 6 поступает в запоминающее устройство 5, как в качестве основы платежного сертификата, так и в качестве подписи нулевого уровня платежного сертификата.

При произвольной операции пополнения платежного устройства 2 подпись платежного сертификата по линии 13 поступает в блок 7, где происходит маскировка подписи платежного сертификата формированием, посредством блока 8, денежного запроса, включающего замаскированную подпись платежного сертификата. Денежный запрос по линии 14 доставляется в платежный сервер 1, где в блоке 11 происходит его обработка, включающая, в том числе и изготовление денежной подписи для замаскированной подписи платежного сертификата посредством блока 12. Сформированный в блоке 11 ответ оператора на денежный запрос поступает по линии 15 в платежное устройство 2, где посредством блока 9 происходит демаскировка содержащихся в ответе на денежный запрос данных для демаскировки. Демаскированные данные по линии 10 поступают в запоминающее устройство 6 в качестве подписи платежного сертификата более высокого уровня.

При проведении платежной операции в блоке 16 платежного устройства 2 формируется платежное поручение плательщика, подписанное секретным ключом платеж-

ного сертификата. По линии 22 платежное поручение плательщика поступает в приемное устройство 3, где в блоке 17 формируется платежное поручение получателя платежа, включающее платежное поручение плательщика. По линии 23 платежное поручение получателя платежа поступает в платежный сервер 1, где посредством блока 19 проводится платежная операция, при которой счет получателя платежа, хранящийся в базе данных счетов 21, кредитруется из средств платежного счета, хранящегося в базе данных платежных счетов 20. При этом, считывание и модификация записей платежного счета и счета получателя платежа осуществляется по линиям 24 и 25, соответственно. Сформированный в блоке 19 ответ оператора на платежное поручение получателя платежа, включающий квитанцию получателя платежа, подписанную секретным ключом оператора, по линии 26 поступает в блок 18 приемного устройства 3, где происходит проверка подписанной квитанции получателя платежа, завершающая проведение платежной операции.

Варианты осуществления изобретения

При осуществлении изобретения по каждому из вариантов заявленного способа проведения платежей пополнение платежного устройства может происходить за счет средств промежуточного плательщика. В этом случае плательщик при пополнении своего платежного устройства доставляет замаскированные данные промежуточному плательщику, который производит их дополнительную маскировку и, соответственно, демаскировку полученных от банка данных для демаскировки.

При необходимости получатель платежа также может осуществлять контроль над принимаемыми платежами. Такой контроль предназначен для того, чтобы никто не мог зачислить деньги на счет получателя платежа помимо его воли. Для осуществления такого контроля платежное поручение получателя платежа доставляют в платежный сервер вместе с его подписью секретным ключом счета получателя платежа, причем при проведении платежной операции осуществляют проверку правильности подписи для платежного поручения получателя платежа. Помимо этого, при формировании платежных поручений плательщика и получателя платежа в эти платежные поручения включают условия платежа, а при проведении платежной операции в платежном сервере контролируют соответствие условий платежа, содержащихся в платежных поручениях плательщика и получателя платежа. В частности, в платежном устройстве при формировании платежных данных, а в приемном устройстве при формировании платежного поручения получателя платежа производят обработку данных обязательства получателя платежа по платежу одной и той же односторонней функцией, причем данные, полученные при этой обработке, включают как в платежные данные, так и в платежное поручение получателя платежа в качестве части условий платежа.

Надежность проведения платежей по каждому из вариантов, в частности, обеспечена тем, что при ошибках работы коммуникационных сетей при проведении вовлеченных в проведение платежа операций, такие операции могут быть повторены до их успешного завершения без ущерба для вовлеченных сторон.

В качестве источника пополнения при операции пополнения платежного устройства может быть использован счет плательщика, который предварительно прокредитован в ходе ранее проведенной платежной операции, в которой плательщик, в свою

очередь, играл роль получателя платежа.

При проведении платежной операции в качестве плательщика может выступать получатель платежа. Такую платежную операцию можно использовать для перевода ценностей из платежного устройства на счет плательщика.

- 5 Слишком быстрый рост числа баз данных оператора, хранящих информацию о платежных сертификатах, может быть предотвращен как взиманием платы за пополнение платежного устройства, так и платой за открытие платежного счета, связанного с платежным сертификатом.

- 10 Денежные обязательства оператора, связанные с платежными сертификатами, могут быть выражены в различных валютах, а проведение как платежной операции, так и операции пополнения платежного устройства может быть совмещено с операцией конвертации из одной валюты в другую.

- 15 Для усиления безопасности участников платежной системы могут быть введены некоторые ограничения как на величину однократного пополнения платежного устройства, так и на общую сумму расходов источника пополнения за определенный период времени.

- 20 Обмен сообщениями между приемным устройством и платежным сервером, платежным устройством и платежным сервером, приемным устройством и платежным устройством, может происходить в интерактивном режиме. В частности, денежный запрос, платежные данные, платежное поручение получателя платежа и другие данные, могут быть доставлены их адресату порциями.

Процедура признания оператором платежной системы своих обязательств по платежному сертификату, помимо проверки собственной подписи для сертификата, может включать проверку срока годности и иных данных.

- 25 Кроме того, полученные при пополнении платежного устройства данные для демаскировки вместе данными, позволяющими осуществить такую демаскировку, могут быть использованы в качестве денежной подписью платежного сертификата, так как позволяют убедить третью сторону в наличии обязательств оператора.

Промышленная применимость

- 30 Изобретение может быть использовано в электронных системах массового обслуживания, в особенности таких, где требуются платежи по открытым коммуникационным сетям. В том числе, изобретение может быть использовано для организации платежных систем, торговых систем, сервисных центров и во многих иных областях. В частности, изобретение может быть использовано в работе банков и банковских систем, для организации магазинов, торговли ценными бумагами, лотерей и т.п.
- 35

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Способ проведения платежей, заключающийся в проведении пополнения платежного устройства посредством операции первичного наполнения платежного сертификата, при которой в платежном устройстве создают основу платежного сертификата и получают подпись платежного сертификата посредством изготовления вслепую денежной подписи оператора, проведении операции открытия счета получателя платежа, проведении платежной операции, при которой подпись и идентификатор основы платежного сертификата включают в платежные данные, доставляемые в приемное устройство, посредством которого формируют платежное поручение получателя платежа, включающее подпись и идентификатор основы платежного сертификата, доставляют сформированное платежное поручение получателя платежа в платежный сервер, в котором по отсутствию информации об использованности платежного сертификата по правильности доставленной подписи платежного сертификата осуществляют кредитование счета получателя платежа на основе его платежного поручения и формируют ответ оператора на платежное поручение получателя платежа, по которому судят о проведении платежа, *отличающийся тем, что* в основу платежного сертификата включают идентификатор открытого ключа, соответствующего произвольному секретному ключу плательщика, причем открытый ключ принимают в качестве открытого ключа, а секретный ключ плательщика принимают в качестве секретного ключа платежного сертификата, в платежные данные включают подписанное секретным ключом платежного сертификата платежное поручение плательщика, в которое включают сведения о получателе платежа и идентификатор основы платежного сертификата, кредитование счета получателя платежа осуществляют по правильности подписи для платежного поручения плательщика.
2. Способ по п. 1, отличающийся тем, что при проведении платежной операции подписанное платежное поручение плательщика заносят в информационное хранилище оператора.
3. Способ по п. 1, отличающийся тем, что при пополнении платежного устройства формируют денежный запрос, включающий данные для изготовления вслепую денежной подписи, и доставляют его в платежный сервер, в котором по денежному запросу определяют источник и сумму пополнения, создают при изготовлении вслепую денежной подписи данные для демаскировки обработкой содержащихся в запросе данных для изготовления вслепую денежной подписи соответствующим сумме пополнения денежным секретным ключом, после чего в платежном устройстве демаскировкой изготавливают подпись платежного сертификата.
4. Способ по п. 3, отличающийся тем, что при пополнении платежного устройства посредством операции первичного наполнения платежного сертификата в формируемый денежный запрос в качестве данных для изготовления вслепую денежной подписи включают замаскированный идентификатор созданной основы платежного сертификата.
5. Способ по п. 1, отличающийся тем, что при проведении платежной операции в ответ оператора на платежное поручение получателя платежа включают квитанцию получателя платежа, подписанную произвольным секретным ключом оператора, а о проведении платежа для получателя платежа судят по правильности подписи для

квитанции получателя платежа.

6. Способ по п. 1, отличающийся тем, что при проведении платежной операции в приемном устройстве по ответу оператора на платежное поручение получателя платежа, формируют и доставляют в платежное устройство данные, по которым судят о
5 проведении платежа для плательщика.

7. Способ по п. 6, отличающийся тем, что при проведении платежной операции в ответ оператора на платежное поручение получателя платежа и в данные, доставляемые в платежное устройство, включают квитанцию плательщика, подписанную произвольным секретным ключом оператора, а о проведении платежа для платель-
10 щика судят по правильности подписи для квитанции плательщика.

8. Способ по п. 7, отличающийся тем, что перед включением в ответ оператора на платежное поручение получателя платежа квитанцию плательщика шифруют произвольным шифровальным ключом плательщика.

9. Способ по п. 1, отличающийся тем, что при проведении операций с платежным сертификатом в качестве идентификатора основы платежного сертификата используют преобразованный посредством произвольной односторонней функции откры-
15 тый ключа платежного сертификата.

10. Способ по п. 1, отличающийся тем, что при проведении операций с платежным сертификатом в качестве идентификатора открытого ключа платежного сертификата используют открытый ключ платежного сертификата.
20

11. Способ по п. 1, отличающийся тем, что при пополнении платежного устройства осуществляют проверку правильности изготовленной подписи платежного сертификата.

12. Способ по п. 1, отличающийся тем, что при проведении операции открытия сче-
25 та в качестве секретного ключа счета принимают произвольный секретный ключ, а открытый ключ, соответствующий секретному ключу счета доставляют в платежный сервер и принимают в качестве открытого ключа открываемого счета.

13. Способ по п. 1, отличающийся тем, что в платежное поручение плательщика включают условия платежа.

14. Способ по п. 13, отличающийся тем, что в условия платежа, содержащиеся в пла-
30 тежном поручении плательщика, включают данные обязательства получателя платежа по платежу.

15. Способ по п. 14, отличающийся тем, что перед проведением платежной операции данные обязательства получателя платежа по платежу подписывают произвольным
35 секретным ключом получателя платежа, а плательщик до платежной операции проверяет подпись получателя платежа для данных обязательства получателя платежа.

16. Способ по п. 13, отличающийся тем, что в платежном устройстве при формиро-
вании платежных данных производят обработку данных обязательства получателя платежа по платежу произвольной односторонней функцией, а данные, полученные
40 при этой обработке, включают в платежное поручение плательщика в качестве условий платежа.

17. Способ по п. 1, отличающийся тем, что перед включением в платежные данные платежное поручение плательщика шифруют произвольным открытым шифроваль-
ным ключом оператора.

18. Способ по п. 1, отличающийся тем, что при пополнении платежного устройства в качестве источника пополнения используют счет плательщика.
19. Способ по п. 1, отличающийся тем, что при пополнении платежного устройства в качестве источника пополнения используют банковскую карточку.
- 5 20. Способ по п. 1, отличающийся тем, что при проведении платежной операции в качестве плательщика выступает получатель платежа.
21. Способ по п. 1, отличающийся тем, что при проведении платежной операции в платежное устройство возвращают часть стоимости платежного сертификата.
22. Способ по п. 1, отличающийся тем, что пополнение платежного устройства осуществляют из средств промежуточного плательщика.
- 10 23. Способ по п. 22, отличающийся тем, что при пополнении платежного устройства данные, замаскированные в платежном устройстве при изготовлении вслепую денежной подписи оператора, подвергают дополнительной маскировке в платежном устройстве промежуточного плательщика.

24. Способ проведения платежей, заключающийся в проведении пополнения платежного устройства посредством операции первичного наполнения платежного сертификата, при которой в платежном устройстве создают основу платежного сертификата и получают подпись платежного сертификата посредством изготовления вслепую денежной подписи оператора, проведении операции открытия счета получателя платежа, проведении платежной операции, при которой подпись и идентификатор основы платежного сертификата включают в платежные данные, доставляемые в приемное устройство, посредством которого формируют платежное поручение получателя платежа, включающее подпись и идентификатор основы платежного сертификата, доставляют сформированное платежное поручение получателя платежа в платежный сервер, в котором по отсутствию информации об использованности платежного сертификата по правильности доставленной подписи платежного сертификата осуществляют кредитование счета получателя платежа на основе его платежного поручения и формируют ответ оператора на платежное поручение получателя платежа, по которому судят о проведении платежа, *отличающийся тем, что* в основу платежного сертификата включают идентификатор открытого ключа, соответствующего произвольному секретному ключу плательщика, причем открытый ключ принимают в качестве открытого ключа, а секретный ключ плательщика принимают в качестве секретного ключа платежного сертификата, проводят пополнение платежного устройства посредством операции пополнения платежного сертификата, при которой изготавливают вслепую денежную подпись оператора для уже имеющейся в платежном устройстве подписи платежного сертификата, в платежные данные включают подписанное секретным ключом платежного сертификата платежное поручение плательщика, в которое включают сведения о получателе платежа и идентификатор основы платежного сертификата, кредитование счета получателя платежа осуществляют по правильности подписи для платежного поручения плательщика.
25. Способ по п. 24, отличающийся тем, что при пополнении платежного устройства формируют денежный запрос, включающий данные для изготовления вслепую денежной подписи, и доставляют его в платежный сервер, в котором по денежному запросу определяют источник и сумму пополнения, создают при изготовлении вслепую денежной подписи данные для демаскировки обработкой содержащихся в запросе данных для изготовления вслепую денежной подписи соответствующим сумме пополнения денежным секретным ключом, после чего в платежном устройстве демаскировкой изготавливают подпись платежного сертификата.
26. Способ по п. 25, отличающийся тем, что при пополнении платежного устройства посредством операции первичного наполнения платежного сертификата в формируемый денежный запрос в качестве данных для изготовления вслепую денежной подписи включают замаскированный идентификатор созданной основы платежного сертификата.
27. Способ по п. 25, отличающийся тем, что при пополнении платежного устройства посредством операции пополнения платежного сертификата в формируемый денежный запрос в качестве данных для изготовления вслепую денежной подписи включают замаскированную подпись платежного сертификата.
28. Способ по п. 24, отличающийся тем, что при проведении платежной операции

подписанное платежное поручение плательщика заносят в информационное хранилище оператора.

29. Способ по п. 24, отличающийся тем, что при проведении платежной операции в ответ оператора на платежное поручение получателя платежа включают квитанцию получателя платежа, подписанную произвольным секретным ключом оператора, а о проведении платежа для получателя платежа судят по правильности подписи для квитанции получателя платежа.

30. Способ по п. 24, отличающийся тем, что при проведении платежной операции в приемном устройстве по ответу оператора на платежное поручение получателя платежа формируют и доставляют в платежное устройство данные, по которым судят о проведении платежа для плательщика.

31. Способ по п. 30, отличающийся тем, что при проведении платежной операции в ответ оператора на платежное поручение получателя платежа и в данные, доставляемые в платежное устройство, включают квитанцию плательщика, подписанную произвольным секретным ключом оператора, а о проведении платежа для плательщика судят по правильности подписи для квитанции плательщика.

32. Способ по п. 31, отличающийся тем, что перед включением в ответ оператора на платежное поручение получателя платежа квитанцию плательщика шифруют произвольным шифровальным ключом плательщика.

33. Способ по п. 24, отличающийся тем, что при проведении операций с платежным сертификатом в качестве идентификатора основы платежного сертификата используют преобразованный посредством произвольной односторонней функции открытый ключа платежного сертификата.

34. Способ по п. 24, отличающийся тем, что при проведении операций с платежным сертификатом в качестве идентификатора открытого ключа платежного сертификата используют открытый ключ платежного сертификата.

35. Способ по п. 24, отличающийся тем, что при пополнении платежного устройства осуществляют проверку правильности изготовленной подписи платежного сертификата.

36. Способ по п. 24, отличающийся тем, что при проведении операции открытия счета в качестве секретного ключа счета принимают произвольный секретный ключ, а открытый ключ, соответствующий секретному ключу счета доставляют в платежный сервер и принимают в качестве открытого ключа открываемого счета.

37. Способ по п. 24, отличающийся тем, что в платежное поручение плательщика включают условия платежа.

38. Способ по п. 37, отличающийся тем, что в условия платежа, содержащиеся в платежном поручении плательщика, включают данные обязательства получателя платежа по платежу.

39. Способ по п. 38, отличающийся тем, что перед проведением платежной операции данные обязательства получателя платежа по платежу подписывают произвольным секретным ключом получателя платежа, а плательщик до платежной операции проверяет подпись получателя платежа для данных обязательства получателя платежа.

40. Способ по п. 38, отличающийся тем, что в платежном устройстве при формировании платежных данных производят обработку данных обязательства получателя

платежа по платежу произвольной односторонней функцией, а данные, полученные при этой обработке, включают в платежное поручение плательщика в качестве условий платежа.

- 5 41. Способ по п. 24, отличающийся тем, что перед включением в платежные данные платежное поручение плательщика шифруют произвольным открытым шифровальным ключом оператора.
42. Способ по п. 24, отличающийся тем, что при пополнении платежного устройства в качестве источника пополнения используют счет плательщика.
- 10 43. Способ по п. 24, отличающийся тем, что при пополнении платежного устройства в качестве источника пополнения используют банковскую карточку.
44. Способ по п. 24, отличающийся тем, что при проведении платежной операции в качестве плательщика выступает получатель платежа.
45. Способ по п. 24, отличающийся тем, что при проведении платежной операции в платежное устройство возвращают часть стоимости платежного сертификата.
- 15 46. Способ по п. 24, отличающийся тем, что пополнение платежного устройства осуществляют из средств промежуточного плательщика.
47. Способ по п. 46, отличающийся тем, что при пополнении платежного устройства данные, замаскированные в платежном устройстве при изготовлении вслепую денежной подписи оператора, подвергают дополнительной маскировке в платежном устройстве промежуточного плательщика.
- 20

48. Способ проведения платежей, заключающийся в проведении пополнения платежного устройства посредством операции первичного наполнения платежного сертификата, при которой в платежном устройстве создают основу платежного сертификата и получают подпись платежного сертификата посредством изготовления
- 5 вслепую денежной подписи оператора, проведении операции открытия счета получателя платежа, проведении платежной операции, при которой идентификатор основы платежного сертификата включают в платежные данные, доставляемые в приемное устройство, посредством которого формируют платежное поручение получателя платежа, включающее полученный от плательщика идентификатор основы платеж-
- 10 ного сертификата, доставляют сформированное платежное поручение получателя платежа в платежный сервер, в котором осуществляют кредитование счета получателя платежа на основе его платежного поручения, формируют ответ оператора на платежное поручение получателя платежа, по которому судят о проведении платежа, *отличающийся тем, что* в основу платежного сертификата включают идентифика-
- 15 тор открытого ключа, соответствующего произвольному секретному ключу плательщика, причем открытый ключ принимают в качестве открытого ключа, а секретный ключ плательщика принимают в качестве секретного ключа платежного сертификата, открывают связанный с основой платежного сертификата платежный счет, осуществляют операцию кредитования платежного счета, при которой в платежный
- 20 сервер доставляют подпись платежного сертификата, уровень которой выбирают произвольно в пределах уровня платежного сертификата, а кредитование платежного счета осуществляют в соответствии с превышением уровня доставленной подписи над уровнем платежного счета, в платежные данные включают подписанное секретным ключом платежного сертификата платежное поручение плательщика, в которое
- 25 включают сведения о получателе платежа и идентификатор основы платежного сертификата, кредитование счета получателя платежа осуществляют по правильности подписи для платежного поручения плательщика из средств платежного счета.
49. Способ по п. 48, отличающийся тем, что связанный с основой платежного сертификата платежный счет открывают при проведении платежной операции.
- 30 50. Способ по п. 48, отличающийся тем, что операцию кредитования платежного счета осуществляют при платежной операции.
51. Способ по п. 48, отличающийся тем, что при проведении платежной операции подписанное платежное поручение плательщика заносят в информационное храни-
- 35 лище оператора.
52. Способ по п. 48, отличающийся тем, что при пополнении платежного устройства формируют денежный запрос, включающий данные для изготовления вслепую денежной подписи, и доставляют его в платежный сервер, в котором по денежному за-
- 40 просу определяют источник и сумму пополнения, создают при изготовлении вслепую денежной подписи данные для демаскировки обработкой содержащихся в запросе данных для изготовления вслепую денежной подписи соответствующим сум-
- ме пополнения денежным секретным ключом, после чего в платежном устройстве демаскировкой изготавливают подпись платежного сертификата.
53. Способ по п. 52, отличающийся тем, что при пополнении платежного устройства посредством операции первичного наполнения платежного сертификата в форми-

руемый денежный запрос в качестве данных для изготовления вслепую денежной подписи включают замаскированный идентификатор созданной основы платежного сертификата.

5 54. Способ п. 48, отличающийся тем, что при проведении платежной операции в ответ оператора на платежное поручение получателя платежа включают квитанцию получателя платежа, подписанную произвольным секретным ключом оператора, а о проведении платежа для получателя платежа судят по правильности подписи для квитанции получателя платежа.

10 55. Способ п. 48, отличающийся тем, что при проведении платежной операции в приемном устройстве по ответу оператора на платежное поручение получателя платежа, формируют и доставляют в платежное устройство данные, по которым судят о проведении платежа для плательщика.

15 56. Способ по п. 55, отличающийся тем, что при проведении платежной операции в ответ оператора на платежное поручение получателя платежа и в данные, доставляемые в платежное устройство, включают квитанцию плательщика, подписанную произвольным секретным ключом оператора, а о проведении платежа для плательщика судят по правильности подписи для квитанции плательщика.

20 57. Способ по п. 56, отличающийся тем, что перед включением в ответ оператора на платежное поручение получателя платежа квитанцию плательщика шифруют произвольным шифровальным ключом плательщика.

58. Способ по п. 48, отличающийся тем, что при проведении операций с платежным сертификатом в качестве идентификатора основы платежного сертификата используют преобразованный посредством произвольной односторонней функции открытый ключа платежного сертификата.

25 59. Способ по п. 48, отличающийся тем, что при проведении операций с платежным сертификатом в качестве идентификатора открытого ключа платежного сертификата используют открытый ключ платежного сертификата.

30 60. Способ по п. 48, отличающийся тем, что при операции пополнения платежного устройства осуществляют проверку правильности изготовленной подписи платежного сертификата.

61. Способ по п. 48, отличающийся тем, что при проведении операции открытия счета в качестве секретного ключа счета принимают произвольный секретный ключ, а открытый ключ, соответствующий секретному ключу счета доставляют в платежный сервер и принимают в качестве открытого ключа открываемого счета.

35 62. Способ по п. 48, отличающийся тем, что в платежное поручение плательщика включают условия платежа.

63. Способ по п. 62, отличающийся тем, что в условия платежа, содержащиеся в платежном поручении плательщика, включают данные обязательства получателя платежа по платежу.

40 64. Способ по п. 63, отличающийся тем, что перед проведением платежной операции данные обязательства получателя платежа по платежу подписывают произвольным секретным ключом получателя платежа, а плательщик до платежной операции проверяет подпись получателя платежа для данных обязательства получателя платежа.

65. Способ по п. 62, отличающийся тем, что в платежном устройстве при формиро-

вании платежных данных производят обработку данных обязательства получателя платежа по платежу произвольной односторонней функцией, а данные, полученные при этой обработке, включают в платежное поручение плательщика в качестве условий платежа.

- 5 66. Способ по п. 48, отличающийся тем, что перед включением в платежные данные платежное поручение плательщика шифруют произвольным открытым шифровальным ключом оператора.
67. Способ по п. 48, отличающийся тем, что при операции пополнения платежного устройства в качестве источника пополнения используют счет плательщика.
- 10 68. Способ по п. 48, отличающийся тем, что при операции пополнения платежного устройства в качестве источника пополнения используют банковскую карточку.
69. Способ по п. 48, отличающийся тем, что при проведении платежной операции в качестве плательщика выступает получатель платежа.
70. Способ по п. 48, отличающийся тем, что при проведении платежной операции в
- 15 платежное устройство возвращают часть стоимости платежного сертификата.
71. Способ по п. 48, отличающийся тем, что при операции пополнения платежного устройства в качестве источника пополнения используют платежный счет, связанный с основой одного из платежных сертификатов.
72. Способ по п. 48, отличающийся тем, что пополнение платежного устройства осуществляют из средств промежуточного плательщика.
- 20 73. Способ по п. 72, отличающийся тем, что при пополнении платежного устройства данные, замаскированные в платежном устройстве при изготовлении вслепую денежной подписи оператора, подвергают дополнительной маскировке в платежном устройстве промежуточного плательщика.

74. Способ проведения платежей, заключающийся в проведении пополнения платежного устройства посредством операции первичного наполнения платежного сертификата, при которой в платежном устройстве создают основу платежного сертификата и получают подпись платежного сертификата посредством изготовления
- 5 вслепую денежной подписи оператора, проведении операции открытия счета получателя платежа, проведении платежной операции, при которой идентификатор основы платежного сертификата включают в платежные данные, доставляемые в приемное устройство, посредством которого формируют платежное поручение получателя платежа, включающее полученный от плательщика идентификатор основы платеж-
- 10 ного сертификата, доставляют сформированное платежное поручение получателя платежа в платежный сервер, в котором осуществляют кредитование счета получателя платежа на основе его платежного поручения, формируют ответ оператора на платежное поручение получателя платежа, по которому судят о проведении платежа, *отличающийся тем, что* в основу платежного сертификата включают идентифика-
- 15 тор открытого ключа, соответствующего произвольному секретному ключу плательщика, причем открытый ключ принимают в качестве открытого ключа, а секретный ключ плательщика принимают в качестве секретного ключа платежного сертификата, проводят операцию пополнения платежного устройства посредством операции пополнения платежного сертификата, проводят операцию пополнения платеж-
- 20 ного устройства посредством операции пополнения платежного сертификата, при которой изготавливают вслепую денежную подпись оператора для уже имеющейся в платежном устройстве подписи платежного сертификата, открывают связанный с основой платежного сертификата платежный счет, осуществляют операцию кредитования платежного счета, при которой в платежный сервер доставляют подпись
- 25 платежного сертификата, уровень которой выбирают произвольно в пределах уровня платежного сертификата, а кредитование платежного счета осуществляют в соответствии с превышением уровня доставленной подписи над уровнем платежного счета, в платежные данные включают подписанное секретным ключом платежного сертификата платежное поручение плательщика, в которое включают сведения о получа-
- 30 теле платежа и идентификатор основы платежного сертификата, кредитование счета получателя платежа осуществляют по правильности подписи для платежного поручения плательщика из средств платежного счета.
75. Способ по п. 74, отличающийся тем, что связанный с основой платежного сертификата платежный счет открывают при проведении платежной операции.
- 35 76. Способ по п. 74, отличающийся тем, что операцию кредитования платежного счета осуществляют при платежной операции.
77. Способ по п. 74, отличающийся тем, что при проведении платежной операции подписанное платежное поручение плательщика заносят в информационное храни-
- 40 78. Способ по п. 74, отличающийся тем, что при пополнении платежного устройства формируют денежный запрос, включающий данные для изготовления вслепую денежной подписи, и доставляют его в платежный сервер, в котором по денежному запросу определяют источник и сумму пополнения, создают при изготовлении вслепую денежной подписи данные для демаскировки обработкой содержащихся в за-

просе данных для изготовления вслепую денежной подписи соответствующим сумме пополнения денежным секретным ключом, после чего в платежном устройстве демаскировкой изготавливают подпись платежного сертификата.

5 79. Способ по п. 78, отличающийся тем, что при пополнении платежного устройства посредством операции первичного наполнения платежного сертификата в формируемый денежный запрос в качестве данных для изготовления вслепую денежной подписи включают замаскированный идентификатор созданной основы платежного сертификата.

10 80. Способ по п. 78, отличающийся тем, что при пополнении платежного устройства посредством операции пополнения платежного сертификата в формируемый денежный запрос в качестве данных для изготовления вслепую денежной подписи включают замаскированную подпись платежного сертификата.

15 81. Способ по п. 74, отличающийся тем, что при проведении платежной операции в ответ оператора на платежное поручение получателя платежа включают квитанцию получателя платежа, подписанную произвольным секретным ключом оператора, а о проведении платежа для получателя платежа судят по правильности подписи для квитанции получателя платежа.

20 82. Способ по п. 74, отличающийся тем, что при проведении платежной операции в приемном устройстве по ответу оператора на платежное поручение получателя платежа, формируют и доставляют в платежное устройство данные, по которым судят о проведении платежа для плательщика.

25 83. Способ по п. 82, отличающийся тем, что при проведении платежной операции в ответ оператора на платежное поручение получателя платежа и в данные, доставляемые в платежное устройство, включают квитанцию плательщика, подписанную произвольным секретным ключом оператора, а о проведении платежа для плательщика судят по правильности подписи для квитанции плательщика.

84. Способ по п. 83, отличающийся тем, что перед включением в ответ оператора на платежное поручение получателя платежа квитанцию плательщика шифруют произвольным шифровальным ключом плательщика.

30 85. Способ по п. 74, отличающийся тем, что при проведении операций с платежным сертификатом в качестве идентификатора основы платежного сертификата используют преобразованный посредством произвольной односторонней функции открытый ключа платежного сертификата.

35 86. Способ по п. 74, отличающийся тем, что при проведении операций с платежным сертификатом в качестве идентификатора открытого ключа платежного сертификата используют открытый ключ платежного сертификата.

87. Способ по п. 74, отличающийся тем, что при операции пополнения платежного устройства осуществляют проверку правильности изготовленной подписи платежного сертификата.

40 88. Способ по п. 74, отличающийся тем, что при проведении операции открытия счета в качестве секретного ключа счета принимают произвольный секретный ключ, а открытый ключ, соответствующий секретному ключу счета доставляют в платежный сервер и принимают в качестве открытого ключа открываемого счета.

89. Способ по п. 74, отличающийся тем, что в платежное поручение плательщика

включают условия платежа.

90. Способ по п. 89, отличающийся тем, что в условия платежа, содержащиеся в платежном поручении плательщика, включают данные обязательства получателя платежа по платежу.

5 91. Способ по п. 90, отличающийся тем, что перед проведением платежной операции данные обязательства получателя платежа по платежу подписывают произвольным секретным ключом получателя платежа, а плательщик до платежной операции проверяет подпись получателя платежа для данных обязательства получателя платежа.

10 92. Способ по п. 89, отличающийся тем, что в платежном устройстве при формировании платежных данных производят обработку данных обязательства получателя платежа по платежу произвольной односторонней функцией, а данные, полученные при этой обработке, включают в платежное поручение плательщика в качестве условий платежа.

15 93. Способ по п. 74, отличающийся тем, что перед включением в платежные данные платежное поручение плательщика шифруют произвольным открытым шифровальным ключом оператора.

94. Способ по п. 74, отличающийся тем, что при операции пополнения платежного устройства в качестве источника пополнения используют счет плательщика.

20 95. Способ по п. 74, отличающийся тем, что при операции пополнения платежного устройства в качестве источника пополнения используют банковскую карточку.

96. Способ по п. 74, отличающийся тем, что при проведении платежной операции в качестве плательщика выступает получатель платежа.

97. Способ по п. 74, отличающийся тем, что при проведении платежной операции в платежное устройство возвращают часть стоимости платежного сертификата.

25 98. Способ по п. 74, отличающийся тем, что при операции пополнения платежного устройства в качестве источника пополнения используют платежный счет, связанный с основой одного из платежных сертификатов.

99. Способ по п. 74, отличающийся тем, что пополнение платежного устройства осуществляют из средств промежуточного плательщика.

30 100. Способ по п. 99, отличающийся тем, что при пополнении платежного устройства данные, замаскированные в платежном устройстве при изготовлении вслепую денежной подписи оператора, подвергают дополнительной маскировке в платежном устройстве промежуточного плательщика.

101. Устройство для проведения платежей, содержащее платежное устройство, приемное устройство и платежный сервер, соединенные телекоммуникационными сетями, причем платежное устройство содержит средство для пополнения платежного устройства с использованием изготовления вслепую денежной подписи оператора, а платежный сервер содержит средство для изготовления денежной подписи, отличающееся тем, что платежное устройство дополнительно содержит средство для создания основы платежного сертификата обработкой односторонней функцией открытого ключа платежного сертификата, средство для сохранения созданной основы платежного сертификата в запоминающем устройстве и средство для формирования платежного поручения плательщика, подписанного секретным ключом платежного сертификата, приемное устройство содержит средство для формирования платежного поручения получателя платежа, включающего платежное поручение плательщика, платежный сервер дополнительно содержит средство для проведения платежной операции, средство для обслуживания базы данных платежных счетов и средство для обслуживания базы данных счетов, причем упомянутое средство для проведения платежной операции имеет средство для проверки подписи платежного поручения плательщика и средство для изготовления подписанной квитанции получателя платежа, упомянутое средство для обслуживания базы данных платежных счетов имеет средство для проверки денежной подписи, а средство для пополнения платежного устройства с использованием изготовления вслепую денежной подписи оператора реализовано средством для повышения уровня подписи платежного сертификата.

102. Устройство по п. 101, отличающееся тем, что приемное устройство содержит средство для открытия счета с открытым ключом, а упомянутое средство для обслуживания базы данных счетов имеет средство для открытия счета с открытым ключом.

103. Устройство по п. 101, отличающееся тем, что платежное устройство содержит средство для открытия счета с открытым ключом, а упомянутое средство для обслуживания базы данных счетов имеет средство для открытия счета с открытым ключом.

104. Устройство по п. 101, отличающееся тем, что упомянутое средство для повышения уровня подписи платежного сертификата имеет средство формирования денежного запроса, включающего замаскированную подпись платежного сертификата, средство для демаскировки содержащихся в ответе на денежный запрос данных для демаскировки и средство для занесения результата демаскировки в упомянутое запоминающее устройство, а платежный сервер содержит средство для обработки денежного запроса, причем упомянутое средство для обработки денежного запроса имеет средство для изготовления денежной подписи.

105. Устройство по п. 101, отличающееся тем, что упомянутое средство для обслуживания базы данных платежных счетов имеет средство для открытия платежного счета и средство для кредитования платежного счета.

106. Устройство по п. 101, отличающееся тем, что приемное устройство имеет средство для проверки подписанной квитанции получателя платежа.

107. Устройство по п. 101, отличающееся тем, что упомянутое средство для формирования платежного поручения плательщика, подписанного секретным ключом

платежного сертификата, имеет средство для формирования запроса на кредитование платежного счета.

108. Устройство по п. 101, отличающееся тем, что упомянутое средство для формирования запроса на кредитование платежного счета имеет средство для понижения уровня подписи платежного сертификата.

109. Устройство по п. 101, отличающееся тем, что платежное устройство, приемное устройство и платежный сервер дополнительно снабжены средствами для шифрования исходящих сообщений и средствами для дешифрования входящих сообщений.

ИЗМЕНЁННАЯ ФОРМУЛА ИЗОБРЕТЕНИЯ)

[получена Международным бюро 3 апреля 2000 (3.04.00);
первоначально заявленные пункты 18, 19, 42, 43, 65, 67, 68, 71, 92, 94, 95, 98 и 108 формулы
изобретения изменены; остальные пункты формулы изобретения оставлены без изменений
(14 страниц)]

1. Способ проведения платежей, заключающийся в проведении пополнения платежного устройства посредством операции первичного наполнения платежного сертификата, при которой в платежном устройстве создают основу платежного сертификата и получают подпись платежного сертификата посредством изготовления вслепую денежной подписи оператора, проведении операции открытия счета получателя платежа, проведении платежной операции, при которой подпись и идентификатор основы платежного сертификата включают в платежные данные, доставляемые в приемное устройство, посредством которого формируют платежное поручение получателя платежа, включающее подпись и идентификатор основы платежного сертификата, доставляют сформированное платежное поручение получателя платежа в платежный сервер, в котором по отсутствию информации об использованности платежного сертификата по правильности доставленной подписи платежного сертификата осуществляют кредитование счета получателя платежа на основе его платежного поручения и формируют ответ оператора на платежное поручение получателя платежа, по которому судят о проведении платежа, *отличающийся тем, что* в основу платежного сертификата включают идентификатор открытого ключа, соответствующего произвольному секретному ключу плательщика, причем открытый ключ принимают в качестве открытого ключа, а секретный ключ плательщика принимают в качестве секретного ключа платежного сертификата, в платежные данные включают подписанное секретным ключом платежного сертификата платежное поручение плательщика, в которое включают сведения о получателе платежа и идентификатор основы платежного сертификата, кредитование счета получателя платежа осуществляют по правильности подписи для платежного поручения плательщика.
2. Способ по п. 1, отличающийся тем, что при проведении платежной операции подписанное платежное поручение плательщика заносят в информационное хранилище оператора.
3. Способ по п. 1, отличающийся тем, что при пополнении платежного устройства формируют денежный запрос, включающий данные для изготовления вслепую денежной подписи, и доставляют его в платежный сервер, в котором по денежному запросу определяют источник и сумму пополнения, создают при изготовлении вслепую денежной подписи данные для демаскировки обработкой содержащихся в запросе данных для изготовления вслепую денежной подписи соответствующим сумме пополнения денежным секретным ключом, после чего в платежном устройстве демаскировкой изготавливают подпись платежного сертификата.
4. Способ по п. 3, отличающийся тем, что при пополнении платежного устройства посредством операции первичного наполнения платежного сертификата в формируемый денежный запрос в качестве данных для изготовления вслепую денежной подписи включают замаскированный идентификатор созданной основы платежного сертификата.
5. Способ по п. 1, отличающийся тем, что при проведении платежной операции в ответ оператора на платежное поручение получателя платежа включают квитанцию получателя платежа, подписанную произвольным секретным ключом оператора, а о проведении платежа для получателя платежа судят по правильности подписи для

квитанции получателя платежа.

6. Способ по п. 1, отличающийся тем, что при проведении платежной операции в приемном устройстве по ответу оператора на платежное поручение получателя платежа, формируют и доставляют в платежное устройство данные, по которым судят о
5 проведении платежа для плательщика.

7. Способ по п. 6, отличающийся тем, что при проведении платежной операции в ответ оператора на платежное поручение получателя платежа и в данные, доставляемые в платежное устройство, включают квитанцию плательщика, подписанную произвольным секретным ключом оператора, а о проведении платежа для плательщика судят по правильности подписи для квитанции плательщика.
10

8. Способ по п. 7, отличающийся тем, что перед включением в ответ оператора на платежное поручение получателя платежа квитанцию плательщика шифруют произвольным шифровальным ключом плательщика.

9. Способ по п. 1, отличающийся тем, что при проведении операций с платежным сертификатом в качестве идентификатора основы платежного сертификата используют преобразованный посредством произвольной односторонней функции открытый ключа платежного сертификата.
15

10. Способ по п. 1, отличающийся тем, что при проведении операций с платежным сертификатом в качестве идентификатора открытого ключа платежного сертификата используют открытый ключ платежного сертификата.
20

11. Способ по п. 1, отличающийся тем, что при пополнении платежного устройства осуществляют проверку правильности изготовленной подписи платежного сертификата.

12. Способ по п. 1, отличающийся тем, что при проведении операции открытия счета в качестве секретного ключа счета принимают произвольный секретный ключ, а открытый ключ, соответствующий секретному ключу счета доставляют в платежный сервер и принимают в качестве открытого ключа открываемого счета.
25

13. Способ по п. 1, отличающийся тем, что в платежное поручение плательщика включают условия платежа.

14. Способ по п. 13, отличающийся тем, что в условия платежа, содержащиеся в платежном поручении плательщика, включают данные обязательства получателя платежа по платежу.
30

15. Способ по п. 14, отличающийся тем, что перед проведением платежной операции данные обязательства получателя платежа по платежу подписывают произвольным секретным ключом получателя платежа, а плательщик до платежной операции проверяет подпись получателя платежа для данных обязательства получателя платежа.
35

16. Способ по п. 13, отличающийся тем, что в платежном устройстве при формировании платежных данных производят обработку данных обязательства получателя платежа по платежу произвольной односторонней функцией, а данные, полученные при этой обработке, включают в платежное поручение плательщика в качестве условий платежа.
40

17. Способ по п. 1, отличающийся тем, что перед включением в платежные данные платежное поручение плательщика шифруют произвольным открытым шифровальным ключом оператора.

18. Способ по п. 3, отличающийся тем, что при пополнении платежного устройства в качестве источника пополнения используют счет плательщика.
19. Способ по п. 3, отличающийся тем, что при пополнении платежного устройства в качестве источника пополнения используют банковскую карточку.
- 5 20. Способ по п. 1, отличающийся тем, что при проведении платежной операции в качестве плательщика выступает получатель платежа.
21. Способ по п. 1, отличающийся тем, что при проведении платежной операции в платежное устройство возвращают часть стоимости платежного сертификата.
22. Способ по п. 1, отличающийся тем, что пополнение платежного устройства осу-
- 10 шествляют из средств промежуточного плательщика.
23. Способ по п. 22, отличающийся тем, что при пополнении платежного устройства данные, замаскированные в платежном устройстве при изготовлении вслепую денежной подписи оператора, подвергают дополнительной маскировке в платежном устройстве промежуточного плательщика.

24. Способ проведения платежей, заключающийся в проведении пополнения платежного устройства посредством операции первичного наполнения платежного сертификата, при которой в платежном устройстве создают основу платежного сертификата и получают подпись платежного сертификата посредством изготовления
- 5 вслепую денежной подписи оператора, проведении операции открытия счета получателя платежа, проведении платежной операции, при которой подпись и идентификатор основы платежного сертификата включают в платежные данные, доставляемые в приемное устройство, посредством которого формируют платежное поручение получателя платежа, включающее подпись и идентификатор основы платежного
- 10 сертификата, доставляют сформированное платежное поручение получателя платежа в платежный сервер, в котором по отсутствию информации об использованности платежного сертификата по правильности доставленной подписи платежного сертификата осуществляют кредитование счета получателя платежа на основе его платежного поручения и формируют ответ оператора на платежное поручение получа-
- 15 теля платежа, по которому судят о проведении платежа, *отличающийся тем, что* в основу платежного сертификата включают идентификатор открытого ключа, соответствующего произвольному секретному ключу плательщика, причем открытый ключ принимают в качестве открытого ключа, а секретный ключ плательщика принимают в качестве секретного ключа платежного сертификата, проводят пополнение
- 20 платежного устройства посредством операции пополнения платежного сертификата, при которой изготавливают вслепую денежную подпись оператора для уже имеющейся в платежном устройстве подписи платежного сертификата, в платежные данные включают подписанное секретным ключом платежного сертификата платежное поручение плательщика, в которое включают сведения о получателе платежа и идентификатор основы платежного сертификата, кредитование счета получателя платежа осуществляют по правильности подписи для платежного поручения плательщика.
- 25 25. Способ по п. 24, отличающийся тем, что при пополнении платежного устройства формируют денежный запрос, включающий данные для изготовления вслепую денежной подписи, и доставляют его в платежный сервер, в котором по денежному за-
- 30 просу определяют источник и сумму пополнения, создают при изготовлении вслепую денежной подписи данные для демаскировки обработкой содержащихся в запросе данных для изготовления вслепую денежной подписи соответствующим сум-
- ме пополнения денежным секретным ключом, после чего в платежном устройстве демаскировкой изготавливают подпись платежного сертификата.
- 35 26. Способ по п. 25, отличающийся тем, что при пополнении платежного устройства посредством операции первичного наполнения платежного сертификата в формируемый денежный запрос в качестве данных для изготовления вслепую денежной подписи включают замаскированный идентификатор созданной основы платежного сертификата.
- 40 27. Способ по п. 25, отличающийся тем, что при пополнении платежного устройства посредством операции пополнения платежного сертификата в формируемый денежный запрос в качестве данных для изготовления вслепую денежной подписи включают замаскированную подпись платежного сертификата.
28. Способ по п. 24, отличающийся тем, что при проведении платежной операции

подписанное платежное поручение плательщика заносят в информационное хранилище оператора.

29. Способ по п. 24, отличающийся тем, что при проведении платежной операции в ответ оператора на платежное поручение получателя платежа включают квитанцию получателя платежа, подписанную произвольным секретным ключом оператора, а о проведении платежа для получателя платежа судят по правильности подписи для квитанции получателя платежа.

30. Способ по п. 24, отличающийся тем, что при проведении платежной операции в приемном устройстве по ответу оператора на платежное поручение получателя платежа формируют и доставляют в платежное устройство данные, по которым судят о проведении платежа для плательщика.

31. Способ по п. 30, отличающийся тем, что при проведении платежной операции в ответ оператора на платежное поручение получателя платежа и в данные, доставляемые в платежное устройство, включают квитанцию плательщика, подписанную произвольным секретным ключом оператора, а о проведении платежа для плательщика судят по правильности подписи для квитанции плательщика.

32. Способ по п. 31, отличающийся тем, что перед включением в ответ оператора на платежное поручение получателя платежа квитанцию плательщика шифруют произвольным шифровальным ключом плательщика.

33. Способ по п. 24, отличающийся тем, что при проведении операций с платежным сертификатом в качестве идентификатора основы платежного сертификата используют преобразованный посредством произвольной односторонней функции открытый ключа платежного сертификата.

34. Способ по п. 24, отличающийся тем, что при проведении операций с платежным сертификатом в качестве идентификатора открытого ключа платежного сертификата используют открытый ключ платежного сертификата.

35. Способ по п. 24, отличающийся тем, что при пополнении платежного устройства осуществляют проверку правильности изготовленной подписи платежного сертификата.

36. Способ по п. 24, отличающийся тем, что при проведении операции открытия счета в качестве секретного ключа счета принимают произвольный секретный ключ, а открытый ключ, соответствующий секретному ключу счета доставляют в платежный сервер и принимают в качестве открытого ключа открываемого счета.

37. Способ по п. 24, отличающийся тем, что в платежное поручение плательщика включают условия платежа.

38. Способ по п. 37, отличающийся тем, что в условия платежа, содержащиеся в платежном поручении плательщика, включают данные обязательства получателя платежа по платежу.

39. Способ п. 38, отличающийся тем, что перед проведением платежной операции данные обязательства получателя платежа по платежу подписывают произвольным секретным ключом получателя платежа, а плательщик до платежной операции проверяет подпись получателя платежа для данных обязательства получателя платежа.

40. Способ по п. 38, отличающийся тем, что в платежном устройстве при формировании платежных данных производят обработку данных обязательства получателя

платежа по платежу произвольной односторонней функцией, а данные, полученные при этой обработке, включают в платежное поручение плательщика в качестве условий платежа.

- 5 41. Способ по п. 24, отличающийся тем, что перед включением в платежные данные платежное поручение плательщика шифруют произвольным открытым шифровальным ключом оператора.
42. Способ по п. 25, отличающийся тем, что при пополнении платежного устройства в качестве источника пополнения используют счет плательщика.
43. Способ по п. 25, отличающийся тем, что при пополнении платежного устройства в качестве источника пополнения используют банковскую карточку.
- 10 44. Способ по п. 24, отличающийся тем, что при проведении платежной операции в качестве плательщика выступает получатель платежа.
45. Способ по п. 24, отличающийся тем, что при проведении платежной операции в платежное устройство возвращают часть стоимости платежного сертификата.
- 15 46. Способ по п. 24, отличающийся тем, что пополнение платежного устройства осуществляют из средств промежуточного плательщика.
47. Способ по п. 46, отличающийся тем, что при пополнении платежного устройства данные, замаскированные в платежном устройстве при изготовлении вслепую денежной подписи оператора, подвергают дополнительной маскировке в платежном
- 20 устройстве промежуточного плательщика.

48. Способ проведения платежей, заключающийся в проведении пополнения платежного устройства посредством операции первичного наполнения платежного сертификата, при которой в платежном устройстве создают основу платежного сертификата и получают подпись платежного сертификата посредством изготовления
- 5 вслепую денежной подписи оператора, проведении операции открытия счета получателя платежа, проведении платежной операции, при которой идентификатор основы платежного сертификата включают в платежные данные, доставляемые в приемное устройство, посредством которого формируют платежное поручение получателя платежа, включающее полученный от плательщика идентификатор основы платежного
- 10 сертификата, доставляют сформированное платежное поручение получателя платежа в платежный сервер, в котором осуществляют кредитование счета получателя платежа на основе его платежного поручения, формируют ответ оператора на платежное поручение получателя платежа, по которому судят о проведении платежа, *отличающийся тем, что* в основу платежного сертификата включают идентификатор
- 15 открытого ключа, соответствующего произвольному секретному ключу плательщика, причем открытый ключ принимают в качестве открытого ключа, а секретный ключ плательщика принимают в качестве секретного ключа платежного сертификата, открывают связанный с основой платежного сертификата платежный счет, осуществляют операцию кредитования платежного счета, при которой в платежный
- 20 сервер доставляют подпись платежного сертификата, уровень которой выбирают произвольно в пределах уровня платежного сертификата, а кредитование платежного счета осуществляют в соответствии с превышением уровня доставленной подписи над уровнем платежного счета, в платежные данные включают подписанное секретным ключом платежного сертификата платежное поручение плательщика, в которое
- 25 включают сведения о получателе платежа и идентификатор основы платежного сертификата, кредитование счета получателя платежа осуществляют по правильности подписи для платежного поручения плательщика из средств платежного счета.
49. Способ по п. 48, отличающийся тем, что связанный с основой платежного сертификата платежный счет открывают при проведении платежной операции.
- 30 50. Способ по п. 48, отличающийся тем, что операцию кредитования платежного счета осуществляют при платежной операции.
51. Способ по п. 48, отличающийся тем, что при проведении платежной операции подписанное платежное поручение плательщика заносят в информационное хранилище оператора.
- 35 52. Способ по п. 48, отличающийся тем, что при пополнении платежного устройства формируют денежный запрос, включающий данные для изготовления вслепую денежной подписи, и доставляют его в платежный сервер, в котором по денежному запросу определяют источник и сумму пополнения, создают при изготовлении вслепую денежной подписи данные для демаскировки обработкой содержащихся в за
- 40 просе данных для изготовления вслепую денежной подписи соответствующим сумме пополнения денежным секретным ключом, после чего в платежном устройстве демаскировкой изготавливают подпись платежного сертификата.
53. Способ по п. 52, отличающийся тем, что при пополнении платежного устройства посредством операции первичного наполнения платежного сертификата в форми-

руемый денежный запрос в качестве данных для изготовления вслепую денежной подписи включают замаскированный идентификатор созданной основы платежного сертификата.

54. Способ п. 48, отличающийся тем, что при проведении платежной операции в ответ оператора на платежное поручение получателя платежа включают квитанцию получателя платежа, подписанную произвольным секретным ключом оператора, а о проведении платежа для получателя платежа судят по правильности подписи для квитанции получателя платежа.
55. Способ п. 48, отличающийся тем, что при проведении платежной операции в приемном устройстве по ответу оператора на платежное поручение получателя платежа, формируют и доставляют в платежное устройство данные, по которым судят о проведении платежа для плательщика.
56. Способ по п. 55, отличающийся тем, что при проведении платежной операции в ответ оператора на платежное поручение получателя платежа и в данные, доставляемые в платежное устройство, включают квитанцию плательщика, подписанную произвольным секретным ключом оператора, а о проведении платежа для плательщика судят по правильности подписи для квитанции плательщика.
57. Способ по п. 56, отличающийся тем, что перед включением в ответ оператора на платежное поручение получателя платежа квитанцию плательщика шифруют произвольным шифровальным ключом плательщика.
58. Способ по п. 48, отличающийся тем, что при проведении операций с платежным сертификатом в качестве идентификатора основы платежного сертификата используют преобразованный посредством произвольной односторонней функции открытый ключа платежного сертификата.
59. Способ по п. 48, отличающийся тем, что при проведении операций с платежным сертификатом в качестве идентификатора открытого ключа платежного сертификата используют открытый ключ платежного сертификата.
60. Способ по п. 48, отличающийся тем, что при операции пополнения платежного устройства осуществляют проверку правильности изготовленной подписи платежного сертификата.
61. Способ по п. 48, отличающийся тем, что при проведении операции открытия счета в качестве секретного ключа счета принимают произвольный секретный ключ, а открытый ключ, соответствующий секретному ключу счета доставляют в платежный сервер и принимают в качестве открытого ключа открываемого счета.
62. Способ по п. 48, отличающийся тем, что в платежное поручение плательщика включают условия платежа.
63. Способ по п. 62, отличающийся тем, что в условия платежа, содержащиеся в платежном поручении плательщика, включают данные обязательства получателя платежа по платежу.
64. Способ по п. 63, отличающийся тем, что перед проведением платежной операции данные обязательства получателя платежа по платежу подписывают произвольным секретным ключом получателя платежа, а плательщик до платежной операции проверяет подпись получателя платежа для данных обязательства получателя платежа.
65. Способ по п. 63, отличающийся тем, что в платежном устройстве при формиро-

вании платежных данных производят обработку данных обязательства получателя платежа по платежу произвольной односторонней функцией, а данные, полученные при этой обработке, включают в платежное поручение плательщика в качестве условий платежа.

- 5 66. Способ по п. 48, отличающийся тем, что перед включением в платежные данные платежное поручение плательщика шифруют произвольным открытым шифровальным ключом оператора.
67. Способ по п. 52, отличающийся тем, что при операции пополнения платежного устройства в качестве источника пополнения используют счет плательщика.
- 10 68. Способ по п. 52, отличающийся тем, что при операции пополнения платежного устройства в качестве источника пополнения используют банковскую карточку.
69. Способ по п. 48, отличающийся тем, что при проведении платежной операции в качестве плательщика выступает получатель платежа.
70. Способ по п. 48, отличающийся тем, что при проведении платежной операции в
- 15 платежное устройство возвращают часть стоимости платежного сертификата.
71. Способ по п. 52, отличающийся тем, что при операции пополнения платежного устройства в качестве источника пополнения используют платежный счет, связанный с основой одного из платежных сертификатов.
72. Способ по п. 48, отличающийся тем, что пополнение платежного устройства осуществляют из средств промежуточного плательщика.
- 20 73. Способ по п. 72, отличающийся тем, что при пополнении платежного устройства данные, замаскированные в платежном устройстве при изготовлении вслепую денежной подписи оператора, подвергают дополнительной маскировке в платежном устройстве промежуточного плательщика.

74. Способ проведения платежей, заключающийся в проведении пополнения платежного устройства посредством операции первичного наполнения платежного сертификата, при которой в платежном устройстве создают основу платежного сертификата и получают подпись платежного сертификата посредством изготовления
- 5 вслепую денежной подписи оператора, проведении операции открытия счета получателя платежа, проведении платежной операции, при которой идентификатор основы платежного сертификата включают в платежные данные, доставляемые в приемное устройство, посредством которого формируют платежное поручение получателя платежа, включающее полученный от плательщика идентификатор основы платеж-
- 10 ного сертификата, доставляют сформированное платежное поручение получателя платежа в платежный сервер, в котором осуществляют кредитование счета получателя платежа на основе его платежного поручения, формируют ответ оператора на платежное поручение получателя платежа, по которому судят о проведении платежа, *отличающийся тем, что* в основу платежного сертификата включают идентифика-
- 15 тор открытого ключа, соответствующего произвольному секретному ключу плательщика, причем открытый ключ принимают в качестве открытого ключа, а секретный ключ плательщика принимают в качестве секретного ключа платежного сертификата, проводят операцию пополнения платежного устройства посредством операции пополнения платежного сертификата, проводят операцию пополнения платеж-
- 20 ного устройства посредством операции пополнения платежного сертификата, при которой изготавливают вслепую денежную подпись оператора для уже имеющейся в платежном устройстве подписи платежного сертификата, открывают связанный с основой платежного сертификата платежный счет, осуществляют операцию кредитования платежного счета, при которой в платежный сервер доставляют подпись
- 25 платежного сертификата, уровень которой выбирают произвольно в пределах уровня платежного сертификата, а кредитование платежного счета осуществляют в соответствии с превышением уровня доставленной подписи над уровнем платежного счета, в платежные данные включают подписанное секретным ключом платежного сертификата платежное поручение плательщика, в которое включают сведения о получа-
- 30 теле платежа и идентификатор основы платежного сертификата, кредитование счета получателя платежа осуществляют по правильности подписи для платежного поручения плательщика из средств платежного счета.
75. Способ по п. 74, отличающийся тем, что связанный с основой платежного сертификата платежный счет открывают при проведении платежной операции.
- 35 76. Способ по п. 74, отличающийся тем, что операцию кредитования платежного счета осуществляют при платежной операции.
77. Способ по п. 74, отличающийся тем, что при проведении платежной операции подписанное платежное поручение плательщика заносят в информационное хранилище оператора.
- 40 78. Способ по п. 74, отличающийся тем, что при пополнении платежного устройства формируют денежный запрос, включающий данные для изготовления вслепую денежной подписи, и доставляют его в платежный сервер, в котором по денежному запросу определяют источник и сумму пополнения, создают при изготовлении вслепую денежной подписи данные для демаскировки обработкой содержащихся в за-

просе данных для изготовления вслепую денежной подписи соответствующим сумме пополнения денежным секретным ключом, после чего в платежном устройстве демаскировкой изготавливают подпись платежного сертификата.

- 5 79. Способ по п. 78, отличающийся тем, что при пополнении платежного устройства посредством операции первичного наполнения платежного сертификата в формируемый денежный запрос в качестве данных для изготовления вслепую денежной подписи включают замаскированный идентификатор созданной основы платежного сертификата.
- 10 80. Способ по п. 78, отличающийся тем, что при пополнении платежного устройства посредством операции пополнения платежного сертификата в формируемый денежный запрос в качестве данных для изготовления вслепую денежной подписи включают замаскированную подпись платежного сертификата.
- 15 81. Способ по п. 74, отличающийся тем, что при проведении платежной операции в ответ оператора на платежное поручение получателя платежа включают квитанцию получателя платежа, подписанную произвольным секретным ключом оператора, а о проведении платежа для получателя платежа судят по правильности подписи для квитанции получателя платежа.
- 20 82. Способ по п. 74, отличающийся тем, что при проведении платежной операции в приемном устройстве по ответу оператора на платежное поручение получателя платежа, формируют и доставляют в платежное устройство данные, по которым судят о проведении платежа для плательщика.
- 25 83. Способ по п. 82, отличающийся тем, что при проведении платежной операции в ответ оператора на платежное поручение получателя платежа и в данные, доставляемые в платежное устройство, включают квитанцию плательщика, подписанную произвольным секретным ключом оператора, а о проведении платежа для плательщика судят по правильности подписи для квитанции плательщика.
- 30 84. Способ по п. 83, отличающийся тем, что перед включением в ответ оператора на платежное поручение получателя платежа квитанцию плательщика шифруют произвольным шифровальным ключом плательщика.
- 35 85. Способ по п. 74, отличающийся тем, что при проведении операций с платежным сертификатом в качестве идентификатора основы платежного сертификата используют преобразованный посредством произвольной односторонней функции открытый ключа платежного сертификата.
86. Способ по п. 74, отличающийся тем, что при проведении операций с платежным сертификатом в качестве идентификатора открытого ключа платежного сертификата используют открытый ключ платежного сертификата.
87. Способ по п. 74, отличающийся тем, что при операции пополнения платежного устройства осуществляют проверку правильности изготовленной подписи платежного сертификата.
- 40 88. Способ по п. 74, отличающийся тем, что при проведении операции открытия счета в качестве секретного ключа счета принимают произвольный секретный ключ, а открытый ключ, соответствующий секретному ключу счета доставляют в платежный сервер и принимают в качестве открытого ключа открываемого счета.
89. Способ по п. 74, отличающийся тем, что в платежное поручение плательщика

включают условия платежа.

90. Способ по п. 89, отличающийся тем, что в условия платежа, содержащиеся в платежном поручении плательщика, включают данные обязательства получателя платежа по платежу.

- 5 91. Способ по п. 90, отличающийся тем, что перед проведением платежной операции данные обязательства получателя платежа по платежу подписывают произвольным секретным ключом получателя платежа, а плательщик до платежной операции проверяет подпись получателя платежа для данных обязательства получателя платежа.

- 10 92. Способ по п. 90, отличающийся тем, что в платежном устройстве при формировании платежных данных производят обработку данных обязательства получателя платежа по платежу произвольной односторонней функцией, а данные, полученные при этой обработке, включают в платежное поручение плательщика в качестве условий платежа.

- 15 93. Способ по п. 74, отличающийся тем, что перед включением в платежные данные платежное поручение плательщика шифруют произвольным открытым шифровальным ключом оператора.

94. Способ по п. 78, отличающийся тем, что при операции пополнения платежного устройства в качестве источника пополнения используют счет плательщика.

- 20 95. Способ по п. 78, отличающийся тем, что при операции пополнения платежного устройства в качестве источника пополнения используют банковскую карточку.

96. Способ по п. 74, отличающийся тем, что при проведении платежной операции в качестве плательщика выступает получатель платежа.

97. Способ по п. 74, отличающийся тем, что при проведении платежной операции в платежное устройство возвращают часть стоимости платежного сертификата.

- 25 98. Способ по п. 78, отличающийся тем, что при операции пополнения платежного устройства в качестве источника пополнения используют платежный счет, связанный с основой одного из платежных сертификатов.

99. Способ по п. 74, отличающийся тем, что пополнение платежного устройства осуществляют из средств промежуточного плательщика.

- 30 100. Способ по п. 99, отличающийся тем, что при пополнении платежного устройства данные, замаскированные в платежном устройстве при изготовлении вслепую денежной подписи оператора, подвергают дополнительной маскировке в платежном устройстве промежуточного плательщика.

101. Устройство для проведения платежей, содержащее платежное устройство, приемное устройство и платежный сервер, соединенные телекоммуникационными сетями, причем платежное устройство содержит средство для пополнения платежного устройства с использованием изготовления вслепую денежной подписи оператора, а платежный сервер содержит средство для изготовления денежной подписи, отличающееся тем, что платежное устройство дополнительно содержит средство для создания основы платежного сертификата обработкой односторонней функцией открытого ключа платежного сертификата, средство для сохранения созданной основы платежного сертификата в запоминающем устройстве и средство для формирования платежного поручения плательщика, подписанного секретным ключом платежного сертификата, приемное устройство содержит средство для формирования платежного поручения получателя платежа, включающего платежное поручение плательщика, платежный сервер дополнительно содержит средство для проведения платежной операции, средство для обслуживания базы данных платежных счетов и средство для обслуживания базы данных счетов, причем упомянутое средство для проведения платежной операции имеет средство для проверки подписи платежного поручения плательщика и средство для изготовления подписанной квитанции получателя платежа, упомянутое средство для обслуживания базы данных платежных счетов имеет средство для проверки денежной подписи, а средство для пополнения платежного устройства с использованием изготовления вслепую денежной подписи оператора реализовано средством для повышения уровня подписи платежного сертификата.

102. Устройство по п. 101, отличающееся тем, что приемное устройство содержит средство для открытия счета с открытым ключом, а упомянутое средство для обслуживания базы данных счетов имеет средство для открытия счета с открытым ключом.

103. Устройство по п. 101, отличающееся тем, что платежное устройство содержит средство для открытия счета с открытым ключом, а упомянутое средство для обслуживания базы данных счетов имеет средство для открытия счета с открытым ключом.

104. Устройство по п. 101, отличающееся тем, что упомянутое средство для повышения уровня подписи платежного сертификата имеет средство формирования денежного запроса, включающего замаскированную подпись платежного сертификата, средство для демаскировки содержащихся в ответе на денежный запрос данных для демаскировки и средство для занесения результата демаскировки в упомянутое запоминающее устройство, а платежный сервер содержит средство для обработки денежного запроса, причем упомянутое средство для обработки денежного запроса имеет средство для изготовления денежной подписи.

105. Устройство по п. 101, отличающееся тем, что упомянутое средство для обслуживания базы данных платежных счетов имеет средство для открытия платежного счета и средство для кредитования платежного счета.

106. Устройство по п. 101, отличающееся тем, что приемное устройство имеет средство для проверки подписанной квитанции получателя платежа.

107. Устройство по п. 101, отличающееся тем, что упомянутое средство для формирования платежного поручения плательщика, подписанного секретным ключом

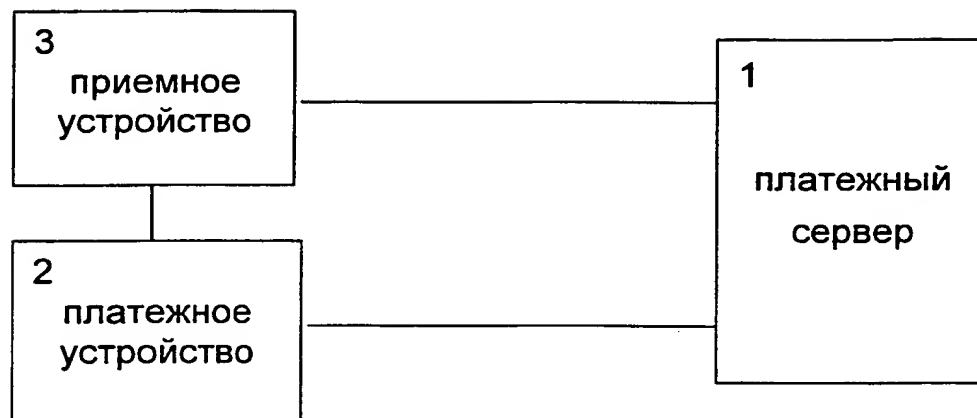
платежного сертификата, имеет средство для формирования запроса на кредитование платежного счета.

108. Устройство по п. 107, отличающееся тем, что упомянутое средство для формирования запроса на кредитование платежного счета имеет средство для понижения уровня подписи платежного сертификата.

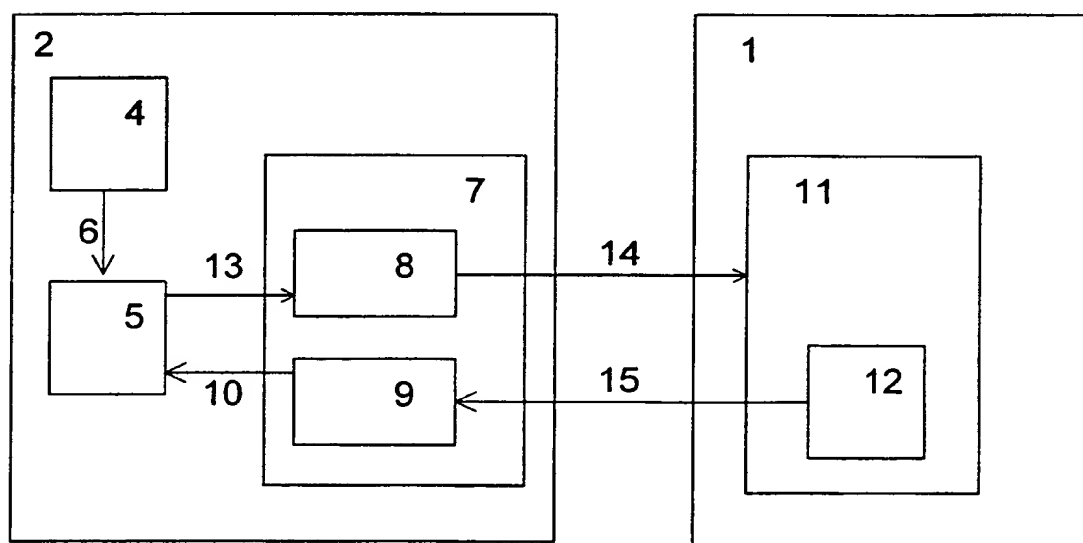
109. Устройство по п. 101, отличающееся тем, что платежное устройство, приемное устройство и платежный сервер дополнительно снабжены средствами для шифрования исходящих сообщений и средствами для дешифрования входящих сообщений.

THIS PAGE BLANK (USPTO)

1/2



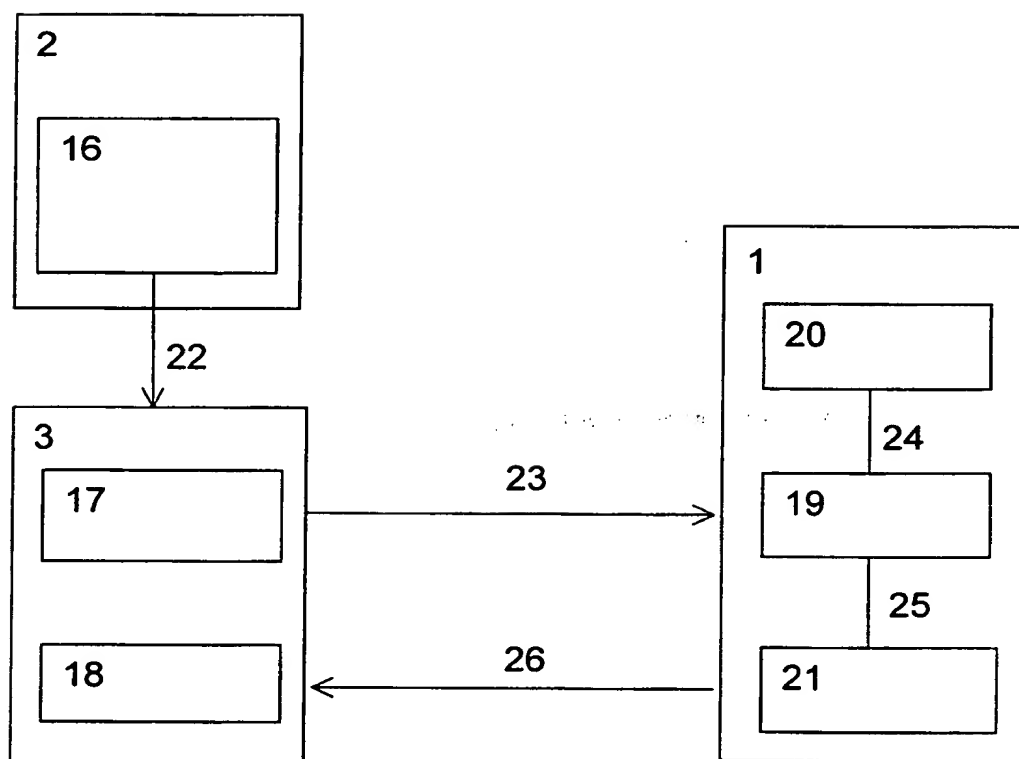
Фиг. 1



Фиг. 2

THIS PAGE BLANK (USPTO)

2/2



Фиг. 3

THIS PAGE BLANK (USPTO)

INTERNATIONAL SEARCH REPORT

Intern al Application No
PCT/RU 99/00264

A. CLASSIFICATION OF SUBJECT MATTER

G07F7/10

According to International Patent Classification (IPC) or to both national classification and IPC ⁷

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G07F, H04L, H04K, G06K

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5748782 A (FERREIRA ET AL.) 05 May 1998, abstract, fig. 1-4, claims 1-22. --	1, 24, 48, 74, 101
A	US 5740246 A (SAITO) 14 April 1998, abstract, fig. 1-5, claims 1-16. --	1, 24, 48, 74, 101
A	US 5768385 A (SIMON, D.R.) 16 June 1998, abstract, fig. 1-7, claims 1-30 (cited in the application). --	1, 24, 48, 74, 101
A	US 5224162 A (OKAMOTO ET AL.) 29 June	1, 24, 48, 74,

☒ Further documents are listed in the continuation of box C.

☐ Patent family members are listed in annex.

* Special categories of cited documents :

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the international filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the international filing date but later than the priority date claimed

- *T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
- *Z* document member of the same patent family

Date of the actual completion of the international search
10 December 1999

Date of mailing of the international search report

02 02 2000

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax (+31-70) 340-3016

Authorized officer

STANGER e.h.

INTERNATIONAL SEARCH REPORT

-2-

Internat'l Application No
PCT/RU 99/00264

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	<p>1993, abstract, fig. 1-12, claims 1-11 (cited in the application). -----</p>	<p>101</p>

ОТЧЁТ О МЕЖДУНАРОДНОМ ПОИСКЕ

Международная заявка №
PCT/RU 99/00264

A. КЛАССИФИКАЦИЯ ПРЕДМЕТА ИЗОБРЕТЕНИЯ: G07F 7/10 Согласно международной патентной классификации (МПК-7)														
B. ОБЛАСТИ ПОИСКА: Проверенный минимум документации (система классификации и индексы) МПК-7: G07F, H04L, H04K, G06K														
Другая проверенная документация в той мере, в какой она включена в поисковые подборки:														
Электронная база данных, использовавшаяся при поиске (название базы и, если, возможно, поисковые термины):														
C. ДОКУМЕНТЫ, СЧИТАЮЩИЕСЯ РЕЛЕВАНТНЫМИ:														
Категория*	Ссылки на документы с указанием, где это возможно, релевантных частей	Относится к пункту №												
A	US 5748782 A (FERREIRA ET AL) 5 мая 1998 (05.05.98), реферат, фиг. 1-4, пункты 1-22 формулы.	1, 24, 48, 74, 101												
A	US 5740246 A (SAITO) 14 апреля 1998 (14.04.98), реферат, фиг. 1-5, пункты 1-16 формулы.	1, 24, 48, 74, 101												
A	US 5768385 (SIMON, D.R.) 16 июня 1998 (16.06.98), реферат, фиг. 1-7, пункты 1-30 формулы, (указан в описании).	1, 24, 48, 74, 101												
A	US 5224162 A (OKAMOTO ET AL) 29 июня 1993 (29.06.93), реферат, фиг. 1-12, пункты 1-11 формулы, (указан в описании).	1, 24, 48, 74, 101												
<div style="display: flex; justify-content: space-between;"> <div> <input type="checkbox"/> последующие документы указаны в продолжении графы C. </div> <div> <input type="checkbox"/> данные о патентах-аналогах указаны в приложении. </div> </div>														
<table border="0"> <tr> <td colspan="2">* Особые категории ссылочных документов:</td> </tr> <tr> <td>A документ, определяющий общий уровень техники</td> <td>T более поздний документ, опубликованный после даты приоритета и приведенный для понимания изобретения</td> </tr> <tr> <td>E более ранний документ, но опубликованный на дату международной подачи или после нее</td> <td>X документ, имеющий наиболее близкое отношение к предмету поиска, порочащий новизну и изобретательский уровень</td> </tr> <tr> <td>O документ, относящийся к устному раскрытию, экспонированию и т.д.</td> <td>Y документ, порочащий изобретательский уровень в сочетании с одним или несколькими документами той же категории</td> </tr> <tr> <td>P документ, опубликованный до даты международной подачи, но после даты испрашиваемого приоритета и т.д.</td> <td>& документ, являющийся патентом-аналогом</td> </tr> <tr> <td>"P" документ, опубликованный до даты международной подачи, но после даты испрашиваемого приоритета.</td> <td>"&" документ, являющийся патентом-аналогом</td> </tr> </table>			* Особые категории ссылочных документов:		A документ, определяющий общий уровень техники	T более поздний документ, опубликованный после даты приоритета и приведенный для понимания изобретения	E более ранний документ, но опубликованный на дату международной подачи или после нее	X документ, имеющий наиболее близкое отношение к предмету поиска, порочащий новизну и изобретательский уровень	O документ, относящийся к устному раскрытию, экспонированию и т.д.	Y документ, порочащий изобретательский уровень в сочетании с одним или несколькими документами той же категории	P документ, опубликованный до даты международной подачи, но после даты испрашиваемого приоритета и т.д.	& документ, являющийся патентом-аналогом	"P" документ, опубликованный до даты международной подачи, но после даты испрашиваемого приоритета.	"&" документ, являющийся патентом-аналогом
* Особые категории ссылочных документов:														
A документ, определяющий общий уровень техники	T более поздний документ, опубликованный после даты приоритета и приведенный для понимания изобретения													
E более ранний документ, но опубликованный на дату международной подачи или после нее	X документ, имеющий наиболее близкое отношение к предмету поиска, порочащий новизну и изобретательский уровень													
O документ, относящийся к устному раскрытию, экспонированию и т.д.	Y документ, порочащий изобретательский уровень в сочетании с одним или несколькими документами той же категории													
P документ, опубликованный до даты международной подачи, но после даты испрашиваемого приоритета и т.д.	& документ, являющийся патентом-аналогом													
"P" документ, опубликованный до даты международной подачи, но после даты испрашиваемого приоритета.	"&" документ, являющийся патентом-аналогом													
Дата действительного завершения международного поиска: 10 декабря 1999 (10.12.99)		Дата отправки настоящего отчёта о международном поиске: 2 февраля 2000 (02.02.00)												
Наименование и адрес Международного поискового органа: Европейское Патентное Ведомство		Уполномоченное лицо: Телефон №												

ANHANG

zum internationalen Recherchen-
bericht über die internationale
Patentanmeldung Nr.

In diesem Anhang sind die Mitglieder
der Patentfamilien der im obenge-
nannten internationalen Recherchenbericht
angeführten Patentdokumente angegeben.
Diese Angaben dienen nur zur Unter-
richtung und erfolgen ohne Gewähr.

ANNEX

to the International Search
Report to the International Patent
Application No.

PCT/RU 99/00264

This Annex lists the patent family
members relating to the patent documents
cited in the above-mentioned inter-
national search report. The Office is
in no way liable for these particulars
which are given merely for the purpose
of information.

ANNEXE

au rapport de recherche inter-
national relatif à la demande de brevet
international n°

La présente annexe indique les
membres de la famille de brevets
relatifs aux documents de brevets cités
dans le rapport de recherche inter-
national visée ci-dessus. Les renseigne-
ments fournis sont donnés à titre indica-
tif et n'engagent pas la responsabilité
de l'Office.

Im Recherchenbericht angeführtes Patentdokument Patent document cited in search report Document de brevet cité dans le rapport de recherche		Datum der Veröffentlichung Publication date Date de publication	Mitglied(er) der Patentfamilie Patent family member(s) Membre(s) de la famille de brevets	Datum der Veröffentlichung Publication date Date de publication
US A	5748782	05-05-1998	EP A1	675614
			FR A1	2718311
			JP A2	7267514
US A	5740246	14-04-1998	EP A2	719045
			EP A3	719045
			JP A2	8288940
US A	5768385	16-06-1998	CA A4	2229206
			EP A2	873615
			EP A4	873615
			WO A2	9709688
			WO A3	9709688
US A	5224162	29-06-1993	DE C0	69210878
			DE T2	69210878
			EP A2	518365
			EP A3	518365
			EP B1	518365
			JP A2	5020344
			JP B2	2631781
			JP A2	4367070
			JP B2	2631776
			JP B2	2631776